NETGEAR

N300 Wireless Gigabit ADSL2+ Modem Router DGN3500

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

June 2010
202-10487-02
v1.0

©2010 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10487-03	v1.0	June 2010	

Table of Contents

Chapter 1 Connecting Your Router to the Internet

Using the Setup Manual 6
Logging In to Your N300 Wireless Modem Router 7
Using the Setup Wizard 9
Viewing or Manually Configuring Your ISP Settings 10
Configuring ADSL Settings 13

Chapter 2 Configuring Your Wireless Network and Security Settings

Planning Your Wireless Network 15
Wireless Placement and Range Guidelines 15
Wireless Security Options 16
Manually Configuring Your Wireless Settings 17
Manually Configuring Your Wireless Security 21
Restricting Wireless Access to Your Network 21
Configuring Mixed WPA-PSK+WPA2-PSK Security 23
Configuring WEP 24
Configuring WPA-802.1x 26
Using Push 'N' Connect (WPS) to Configure Your Wireless Network 27
Using a WPS Button to Add a WPS Client 27
Using PIN Entry to Add a WPS Client 29
Connecting Additional Wireless Devices After WPS Setup 30
Adding More WPS Clients 30
Adding Both WPS and Non-WPS Clients 30
Configuring Advanced WPS Settings 31

Chapter 3 Protecting Your Network

Protecting Access to Your N300 Wireless Modem Router 34
How to Change the Built-In Password 34
Changing the Administrator Login Time-out 35
Viewing Logs of Web Access or Attempted Web Access 36
Blocking Sites 37
Firewall Rules 39
Inbound Rules (Port Forwarding) 40
Outbound Rules (Service Blocking) 42
Order of Precedence for Rules 44
Services 45
Setting Times and Scheduling Firewall Services 47
Setting Your Time Zone 47

Scheduling Firewall Services 48
Configuring E-mail Alerts and Web Access Log Notifications 49

Chapter 4 Managing Your Network

Upgrading the Firmware 52
Manually Checking for Firmware Upgrades 53
Viewing N300 Wireless Modem Router Status Information 55
Connection Status 57
Statistics 58
Viewing a List of Attached Devices 59
Managing the Configuration File 60
Backing Up and Restoring the Configuration 60
Erasing the Configuration 61
Running Diagnostic Utilities and Rebooting the N300 Wireless Modem Router 62
Enabling Remote Management Access 63

Chapter 5 Advanced Configuration

WAN Setup 66
Setting Up a Default DMZ Server 67
Using the N300 Wireless Modem Router as a DHCP Server 70
Address Reservation 70
Configuring LAN Setup 72
Using the N300 Wireless Modem Router as a DHCP Server 73
Address Reservation 74
Dynamic DNS Service 76
Setting up Static Routes 78
Static Route Example 78
Configuring Static Routes 78
Configuring Universal Plug and Play 81
Building Wireless Bridging and Repeating Networks 83
Configuring a Point-to-Point Bridge Configuration 84
Configuring a Repeater with Wireless Client Association 85

Chapter 6 USB Storage

USB Drive Requirements 88
File Sharing Scenarios 89
Sharing Photos with Friends and Family 89
Sharing Large Files with Colleagues 90
USB Storage Basic Settings 91
Editing a Network Folder 93
Configuring USB Storage Advanced Settings 94
Creating a Network Folder 95
Unmounting a USB Drive 97
Specifying Approved USB Devices 98
Connecting to the USB Drive from a Remote Computer 99
Locating the Internet Port IP Address 99

Accessing the Router's USB Drive Remotely Using FTP 99
Connecting to the USB Drive with Microsoft Network Settings 100
Enabling File and Printer Sharing 100

Chapter 7 Troubleshooting

Basic Functioning 102
"Welcome" Page Displays instead of Router Management Interface . . 102
Power LED Is Not On 102
Power LED Is Red 102
LAN or ADSL Port LED Is Not On 103
Window Appears Asking You to Reload Firmware 103
Cannot Log in to the N300 Wireless Modem Router 104
Troubleshooting the ISP Connection 105
ADSL Link 105
Internet LED is Red 106
Obtaining an Internet IP Address 106
Troubleshooting PPPoE or PPPoA 107
Troubleshooting Internet Browsing 107
Resolving a 'Reload Firmware' Message 108
Troubleshooting a TCP/IP Network Using the Ping Utility 109
Testing the LAN Path to Your Router 109
Testing the Path from Your Computer to a Remote Device 110
Restoring the Default Configuration and Password 111
Using the Wireless On/Off and WPS Buttons to Reset the Router 111
Problems with Date and Time 112

Appendix A Technical Specifications

General Specifications 114
Factory Default Configuration 115

Appendix B Related Documents

Appendix C Notification of Compliance

Connecting Your Router to the Internet

1

This chapter describes how to configure your N300 Wireless Modem Router Internet connection. When you install your wireless modem router using the *Resource CD* as described in the *Setup Manual,* these settings are configured automatically for you. This chapter provides instructions on how to log in to the wireless modem router for further configuration.

Note: NETGEAR recommends that Windows OS users use the Smart Wizard™ on the *Resource CD* for initial configuration. Mac and Linux OS users should access the *Setup Manual* on the *Resource CD*.

This chapter includes:

- **Logging In to Your N300 Wireless Modem Router**
- **Using the Setup Wizard**
- **Viewing or Manually Configuring Your ISP Settings**
- **Configuring ADSL Settings**

Using the Setup Manual

For first-time installation of your wireless wireless modem router, refer to the *Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your wireless modem router and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless wireless modem router.

For installation instructions in a language other than English, see the language options on the *Resource CD*.

Logging In to Your N300 Wireless Modem Router

You can log in to the wireless modem router to view or change its settings. Links to Knowledge Base and documentation are also available on the wireless modem router main menu.

Note: Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in ***Related Documents*** in Appendix B.

When you have logged in, if you do not click **Logout**, the wireless modem router waits for 5 minutes after no activity before it automatically logs you out.

To log in to the wireless modem router:

1. Type **http://www./routerlogin.net**, or **http://www.routerlogin.com,** or the wireless modem router's LAN IP address (default is 192.168.0.1) in the address field of your browser, and then press Enter. A login window displays:

Figure 1.

2. Enter **admin** for the wireless modem router user name and your password (or the default, **password**). For information about how to change the password, see ***How to Change the Built-In Password*** on page 34.

Note: The wireless modem router user name and password are not the same as any other user name or password you might use to log in to your Internet connection.

If the wireless modem router has never been configured, the Smart Wizard screen displays. After the wireless modem router has been configured, the Firmware Upgrade assistant will appear.

- **Checking for Firmware Updates screen**. After initial configuration, this screen displays unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.

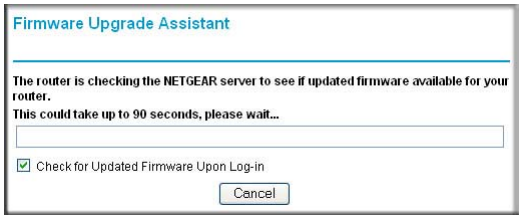

Firmware Upgrade Assistant
The router is checking the NETGEAR server to see if updated firmware available for your router.
This could take up to 90 seconds, please wait...
Check for Updated Firmware Upon Log-in
Cancel

Figure 2.

Note: If the wireless modem router is not configured (is in its factory default state) when you log in, the Setup Wizard displays. See ***Using the Setup Wizard*** on page 9.

If the wireless modem router discovers a newer version of the firmware, you are asked if you want to upgrade to the new firmware (see ***Upgrading the Firmware*** on page 52 for details). If no new firmware is available, the following message displays.

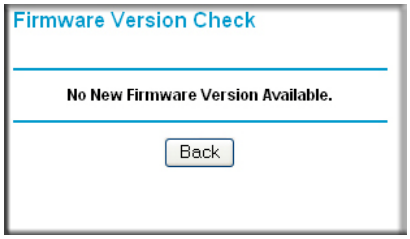


Figure 3.

- **Router Status screen**. The Router Status screen displays if the wireless modem router has not been configured yet or has been reset to its factory default settings. See ***Viewing N300 Wireless Modem Router Status Information*** on page 55.

  You can use the Setup Wizard to automatically detect your Internet connection as described in ***Using the Setup Wizard*** on page 9, or you can bypass the Setup Wizard and manually configure your Internet connection as described in ***Viewing or Manually Configuring Your ISP Settings*** on page 10.

Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Setup Wizard to detect your Internet connection. The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. This feature is not the same as the Smart Wizard on the *Resource CD* that is used for installation.

To use the Setup Wizard:

1. To go to the Setup Wizard screen, from the top of the main menu, select Setup Wizard.

Setup Wizard
Select Country and Language
Country:
UK
Language:
English
Auto-Detect Connection Type
This Setup Wizard can detect the type of Internet connection you have.
Do You want The Smart Setup Wizard To try And detect The connection type now?
Yes.
No. I want to configure The Router myself.
Next

Figure 4.

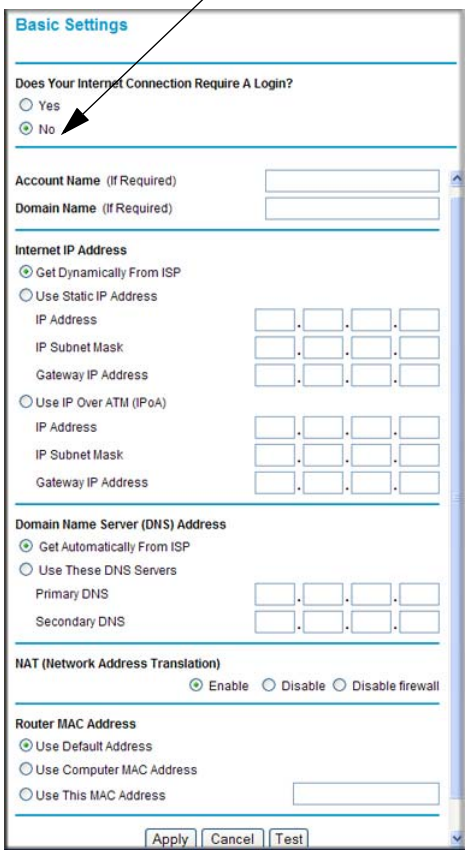
2. Select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.
3. Enter your ISP settings, as needed.
4. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see **Chapter 7**, **Troubleshooting**.

Viewing or Manually Configuring Your ISP Settings

To view or configure the basic settings:

1. Log in to the wireless modem router as described in ***Logging In to Your N300 Wireless Modem Router*** on page 7.
2. Select Basic Settings from the wireless modem router menu to display the Basic Settings screen.

ISP *does not* require login



ISP *does* require login

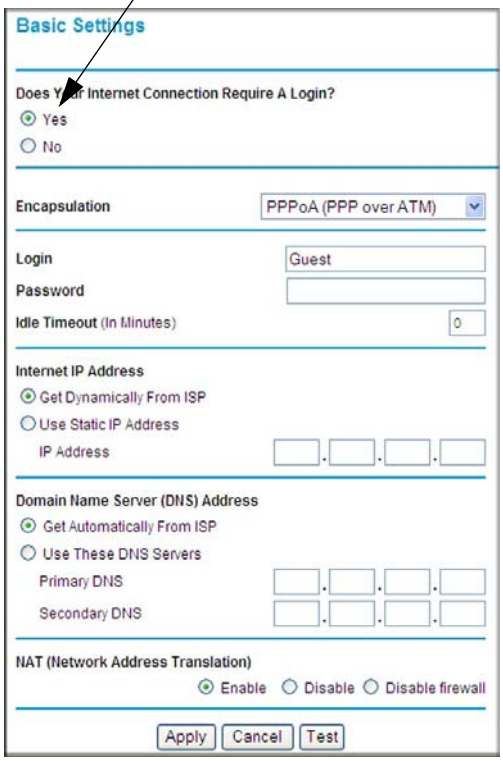


Figure 5.

3. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.
   - **Yes**. If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.
4. Enter the settings for the IP address and DNS server. If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

5. If no login is required, you can specify the MAC Address setting.
6. Click **Apply** to save your settings.
7. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to.

   When your Internet connection is working, you do not need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your wireless modem router automatically logs you in.

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields appear only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields appear only if your ISP requires a login.	Encapsulation	• PPPoE (PPP over Ethernet) • PPPoA (PPP over ATM)
	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password that you use to log in to your ISP.
	Idle Timeout (In minutes)	If you want to change the login time-out, enter a new value in minutes. This determines how long the wireless modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.
Internet IP Address		• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's wireless modem router to which your wireless modem router will connect.
	This field appears only if no login is required.	• **Use IP Over ATM (IPoA)**. Your ISP uses Classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. • **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the wireless modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Settings		Description
NAT (Net Address Translation)		NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices. • **Enable**. Usually NAT is enabled. • **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the wireless modem router uses. Classical routing should be selected only by experienced users[1] • **Disable firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.
These fields appear only if no login is required.	Router MAC Address	The Ethernet MAC address that will be used by the wireless modem router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your wireless modem router to masquerade as that computer by "cloning" its MAC address. • **Use Default Address**. Use the default MAC address. • **Use Computer MAC Address**. The wireless modem router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • **Use This MAC Address**. Enter the MAC address that you want to use.

1 Disabling NAT reboots the wireless modem router and resets its configuration settings to the factory defaults. Disable NAT only if you plan to install the wireless modem router in a setting where you will be manually administering the IP address space on the LAN side of the router.

Configuring ADSL Settings

> **Note:** For information about how to install ADSL filters, see the *Setup Manual*.

NETGEAR recommends that you use the Setup Wizard to automatically detect and configure your ADSL settings. This usually works fine. However, if you have technical experience and are sure of the multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI), you can specify those settings here.

> **Note:** NETGEAR recommends using the Setup Wizard to select the correct country to optimize detection of the ADSL settings.

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting:

1. From the main menu, select ADSL Settings.The ADSL Settings screen displays.

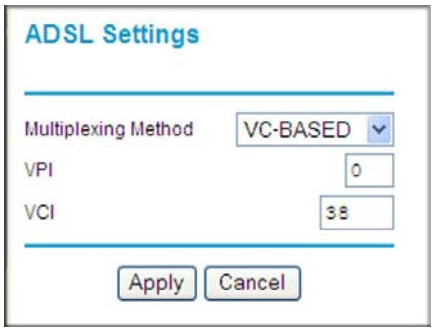


Figure 6.

2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8.
4. For the VCI, type a number between 32 and 65535. The default is 35.
5. Click **Apply**.

Configuring Your Wireless Network and Security Settings

2

This chapter describes how to configure the wireless features of your N300 Wireless Gigabit ADSL2+ Modem Router DGN3500. For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

WARNING!

Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- **Planning Your Wireless Network**
- **Manually Configuring Your Wireless Settings**
- **Manually Configuring Your Wireless Security**
- **Using Push 'N' Connect (WPS) to Configure Your Wireless Network**
- **Connecting Additional Wireless Devices After WPS Setup**

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the modem router is NETGEAR.
  - The wireless mode (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
  - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

  See ***Manually Configuring Your Wireless Security*** on page 21.
- Push 'N' Connect (WPS) automatically implements wireless security on the modem router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the modem router, clicking an on-screen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

  To set up your wireless network using the WPS feature:

  - Use the WPS button on the side of the modem router (there is also an on-screen WPS button), or enter the PIN of the wireless device.
  - Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

  See ***Using Push 'N' Connect (WPS) to Configure Your Wireless Network*** on page 27.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the modem router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your modem router according to the following guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless modem router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

- **Restrict access based on MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless modem router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed (see ***Restricting Wireless Access to Your Network*** on page 21).
- **Turn off the broadcast of the wireless network name SSID**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed (see ***Hiding your wireless network name (SSID)*** on page 21).
- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK (see ***Configuring WEP*** on page 24).
- **WPA-802.1x**. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers (see ***Configuring WPA-802.1x*** on page 26).
- **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise (see ***Configuring Mixed WPA-PSK+WPA2-PSK Security*** on page 23).

For more information about wireless technology, see the link to the online document in ***Virtual Private Networking Basics*** in Appendix B.

Manually Configuring Your Wireless Settings

You can view or manually configure the wireless settings for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.

Note: If you use a wireless computer to change the wireless network name (SSID) or wireless security settings, you will be disconnected when you click **Apply**. To avoid this problem, use a computer with a wired connection to access the modem router.

To view or manually configure the wireless settings:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu. The Wireless Settings screen displays.

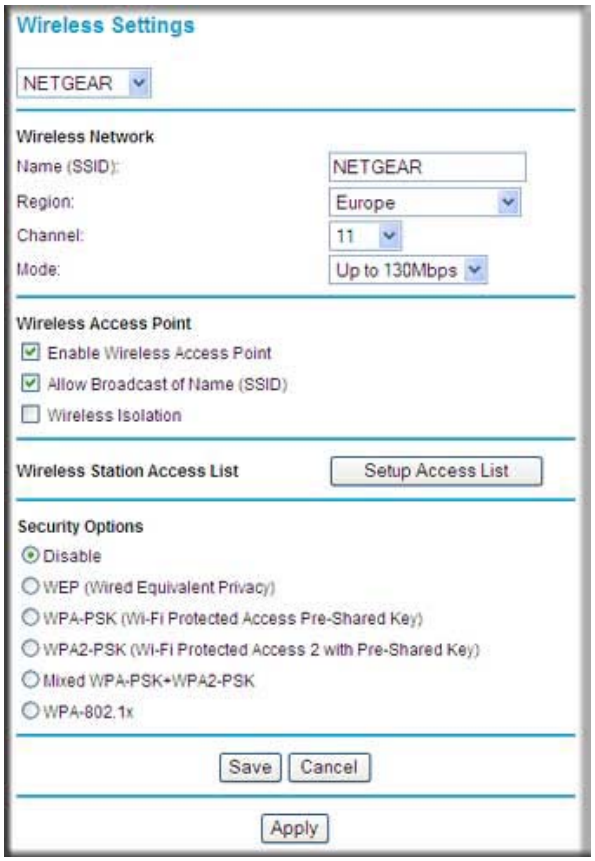


Figure 7.

Table 1 describes the information that is displayed in the Wireless Settings screen.

Note: The SSID of any wireless access adapters must match the SSID you specify in the wireless modem router. If they do not match, you will not get a wireless connection.

3. Select the region in which the wireless modem router will operate.

Note: Up to 270Mbps mode uses two channels, but in this mode only the first channel is listed in the channel pull-down menu. The associated channels in this mode are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. When you select another wireless network mode, the channel pull-down displays all available channels: 1 through 13. However, available wireless channels depend on the selected wireless region.

4. For initial configuration and test, leave the other settings unchanged.
5. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.
6. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and wireless settings I that you specified in the router. Check that they have a wireless link and can obtain an IP address by DHCP from the wireless modem router. If there is interference, adjust the channel.

Table 1. Wireless Settings

Settings	Description
Wireless LAN	Select the wireless LAN that you want to set up. • NETGEAR. This is the primary LAN where you set up the region, channel, mode, and access control (if used). • NETGEAR2 • NETGEAR3 • NETGEAR4
Name (SSID)	This is the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. To join a wireless network, wireless devices use the SSID.
Region	The location where the wireless modem router is used.

Table 1. Wireless Settings

Settings	Description
Mode	Specify which 802.11 data communications protocol is used. You can select one of the following modes: • **Up to 270 Mbps**. Performance mode, using channel expansion to achieve the 270 Mbps data rate. The N300 Wireless Modem Router uses the channel you selected as the primary channel and expands to the secondary channel (primary channel +4 or –4) to achieve a 40 MHz frame-by-frame bandwidth. The N300 Wireless Modem Router detects channel usage and disables frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients. • **Up to 130 Mbps**. Neighbor friendly mode, for reduced interference with neighboring wireless networks. Provides two transmission streams with different data on the same channel at the same time, but also allows 802.11b and 802.11g wireless devices. • **g & b** allows older 802.11g and 802.11b wireless stations to access this wireless network. You might use this mode for a wireless computer using WEP security that does not support WPA-PSK or WPA2-PSK. • **g only** allows only 802.11g wireless stations to access the wireless network.
Channel	The wireless channel fields determine the operating frequency used for the wireless networks. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
Enable Wireless Access Point	• Selected by default, this check box enables the wireless radio, which allows the wireless modem router to work as a wireless access point. • Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting. • The Wireless LED on the front of the modem router displays the current status of the wireless access point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet.
Allow Broadcast of Name (SSID).	Selected by default, the wireless modem router broadcasts its SSID. This makes it easier to select the right wireless network to connect to. If you clear this check mark and click **Apply**, your network name will be hidden. The first time a wireless device connects to it, the SSID must be typed in.
Wireless Isolation	This feature is disabled by default. If you select this check box, then the only way to connect to the wireless modem router will be via cable on the LAN.

Table 1. Wireless Settings

Settings	Description
Wireless Station Access List	This is disabled by default so that any computer configured with the correct wireless network name or SSID can access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. See **Restricting access by MAC address**
Security Options	• **Disable**. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy)**. Use encryption keys and data encryption for data security. Select 64-bit or 128-bit encryption. See ***Configuring WEP*** on page 24. • WPA-PSK (WiFi Protected Access Pre-Shared Key). Allow only computers configured with WPA to connect to the wireless modem router. • WPA2-PSK Wi-Fi Protected Access with 2 Pre-Shared Keys). Allow only computers configured with WPA2 to connect to the wireless modem router. • **Mixed WPA-PSK + WP A2-PSK**. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless modem router. • **WPA-802.1x**. • For WPA or WPA2 configuration, see ***Configuring Mixed WPA-PSK+WPA2-PSK Security*** on page 23.

Manually Configuring Your Wireless Security

To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see ***Using Push 'N' Connect (WPS) to Configure Your Wireless Network*** on page 27).

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID can access your wireless network. For increased security, the wireless modem router provides several ways to restrict wireless access to your network. You can do the following:

- Turn off wireless connectivity completely.
- Restrict access based on the wireless network name (SSID).
- Restrict access based on the Wireless Card Access List.

Turning off wireless connectivity completely

You can completely turn off the wireless connectivity of the wireless modem router by pressing the Wireless On/Off button on the side panel of the wireless modem router. For example, if you use your notebook computer to wirelessly connect to your wireless modem router and you take a business trip, you can turn off the wireless portion of the wireless modem router while you are traveling. Other members of your household who use computers connected to the wireless modem router through Ethernet cables can still use the wireless modem router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.

Hiding your wireless network name (SSID)

By default, the wireless modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Allow Broadcast of Name (SSID)** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not “see” your wireless modem router. You must configure your wireless devices to match the wireless network name (SSID) of the wireless modem router.

WARNING!

The SSID of any wireless access adapters must match the SSID you specify in the wireless modem router. If they do not match, you will not get a wireless connection to the wireless modem router.

Restricting access by MAC address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Awireless modem router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.The Wireless Station Access list determines which wireless hardware devices will be allowed to connect to the wireless modem router.

To restrict access based on MAC addresses:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

Note: If you configure the wireless modem router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the wireless modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

2. In the Wireless Settings screen, under the Wireless Station Access List section, click the **Setup Access List** button. The Wireless Station Access List screen displays:
3. Select the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.
4. Specify which wireless computers you want to allow to access your wireless network.

Figure 8.

- If a computer is connected to the network, you can select it from the Available Wireless Stations list.
- You can copy and paste the MAC addresses from the wireless modem router's Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the wireless modem router. The computer should then appear in the Attached Devices screen.
- If the computer is not connected, you can type in its MAC address. The MAC address is usually printed on the wireless device, or it might appear in the wireless modem router's DHCP table. The MAC address is 12 hexadecimal digits.

5. Click **Add** to add the station to the Trusted Wireless Stations list.

   Tip: If you are using a wireless computer to set up access control, be sure to add your computer to the Trusted Wireless Stations list. Otherwise when you click **Apply** and your changes take effect you will be disconnected from the wireless network.

6. Make sure the **Turn Access Control On** check box is selected, and then click **Apply**.

   Now, only devices on this list will be allowed to wirelessly connect to the wireless modem router. This prevents unauthorized access to your network.

Configuring Mixed WPA-PSK+WPA2-PSK Security

A high-performance client such as the NETGEAR WN511B must connect to the wireless modem router using WPA2-PSK to achieve maximum performance. Wireless clients that connect to the wireless modem router using WPA-PSK run at no more than 802.11g speed. This option allows wireless clients to use either encryption method.

Note: Not all wireless adapters support WPA or WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure Mixed WPA-PSK+WPA2-PSK:

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings below Setup in the main menu of the wireless modem router.
3. Select the **Mixed WPA-PSK+WPA2-PSK** radio button. The Wireless Settings screen expands to include the WPA-PSK.

4. Enter the pre-shared key in the **Network Key** field using between 8 and 63 characters.

   Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.

Note: The procedures to configure WPA-PSK and WPA2-PSK are identical to the procedure to configure Mixed WPA-PSK+WPA2-PSK. The only difference is that you select either the **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)** or **WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)** radio button in step 3.

For details about WPA-802.1x authentication options, see ***Configuring WPA-802.1x*** on page 26.

Configuring WEP

Wired Equivalent Privacy (WEP) security is the most basic and simplest form of wireless security. It is the most often used, but least secure of the available options. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

To configure WEP data encryption:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu.
3. In the Security Options section of the screen, select **WEP (Wired Equivalent Privacy)**. The WEP Security Encryption section displays.

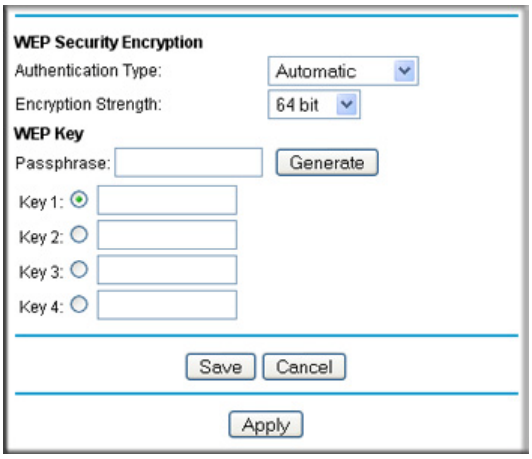


Figure 9.

4. Select the authentication type:
   - **Automatic**.This is the default setting.
   - **Open System**.
   - **Shared Key**.
5. Select the encryption strength setting:
   - **64-bit WEP**.
   - **128-bit WEP**.
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network.
   - Automatic. Enter a word or group of printable characters in the **Passphrase** field and click **Generate**. The four key boxes are automatically populated with key values.
   - Manual. The number of hexadecimal digits that you must enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
7. Select the radio button for the key you want to make active.

   Be sure that you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP allow entry of only one key, which must match the default key you set in the wireless modem router.
8. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.

Note: When configuring the wireless modem router from a wireless computer, if you specify WEP settings, you will lose your wireless connection when you click **Apply**. You must then either configure your wireless adapter to match the wireless modem router WEP settings or access the wireless modem router from a wired computer to make any further changes.

Configuring WPA-802.1x

This version of WPA requires the use of a RADIUS server for authentication. Each user (wireless client) must have a user login on the RADIUS server, and the wireless modem router must have a client login on the RADIUS server. Data transmissions are encrypted using a key that is automatically generated.

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu.
3. In the Security Options section of the screen, select **WPA-802.1x**.
4. In the **Radius Server Name/IP Address** field, enter the name or IP address of the Radius server on your LAN. This is a required field.
5. In the **Radius Port** field, enter the port number used for connections to the Radius server. The default port is 1812.
6. In the **Shared Key** field, enter the value that you want to use for the RADIUS shared key. This key enables the wireless modem router to log in to the RADIUS server and must match the client login value used on the Radius server.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the wireless modem router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the wireless modem router. Look for the symbol on your client device (computers that will connect wirelessly to the wireless modem router are clients). WPS automatically configures the network name (SSID) and wireless security settings for the wireless modem router (if the wireless modem router is in its default state) and broadcasts these settings to the wireless client.

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices. See ***Adding Both WPS and Non-WPS Clients*** on page 30.

A WPS client can be added using the Push Button method or the PIN method.

- **Using the Push Button**. This is the preferred method. See the following section, **Using a WPS Button to Add a WPS Client**.
- **Entering a PIN**. For information about using the PIN method, see ***Using PIN Entry to Add a WPS Client*** on page 29.

Using a WPS Button to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the wireless modem router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the wireless modem router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use the wireless modem router WPS button to add a WPS client:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the wireless modem router main menu, select Add a WPS Client, and then click **Next**. The following screen displays:

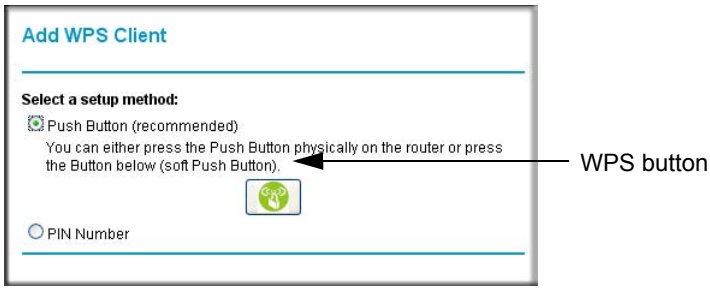

Add WPS Client
Select a setup method:
Push Button (recommended)
You can either press the Push Button physically on the router or press the Button below (soft Push Button).
PIN Number
WPS button

Figure 10.

By default, the **Push Button (recommended)** radio button is selected.

3. Either press the WPS button, or click the on screen button.

   The wireless modem router tries to communicate with the client for 2 minutes.

4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to push or click a WPS button.
5. Go back to the wireless modem router screen to check for a message.
   - While the wireless modem router attempts to connect to a WPS-capable device, the Push 'N' Connect LED on the front blinks green. When the wireless modem router has established a WPS connection, the LED is solid green.
   - If a connection is established, the wireless modem router WPS screen displays a message confirming that the wireless client was successfully added to the wireless network. (The wireless modem router has generated an SSID, implemented WPA/WPA2 wireless security [including a PSK security password] on the wireless modem router, and has sent this configuration to the wireless client.)
6. Note the new SSID and WPA/WPA2 password for the wireless network.

   To access the Internet from any computer connected to your wireless modem router, launch a browser such as Microsoft Internet Explorer. You should see the wireless modem router's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute timeframe, security will not be implemented on the modem router.

Using PIN Entry to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the wireless modem router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the wireless modem router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use a PIN to add a WPS client:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the wireless modem router main menu, select Add a WPS Client (computers that will connect wirelessly to the wireless modem router are clients), and then click **Next**. The Add WPS Client screen displays:

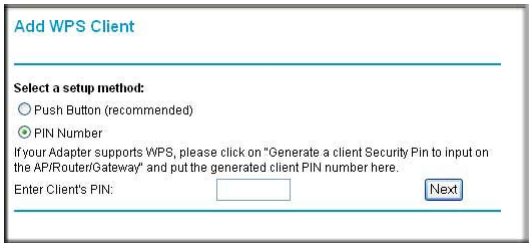

Add WPS Client
Select a setup method:
Push Button (recommended)
PIN Number
If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.
Enter Client's PIN:
Next

Figure 11.

3. Select the **PIN Number** radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. From the wireless modem router Add WPS Client screen, enter the client PIN number, and then click **Next**.
   - The wireless modem router tries to communicate with the client for 4 minutes.
   - The wireless modem router WPS screen displays a message confirming that the client was added to the wireless network. The wireless modem router generates an SSID, and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See ***Manually Configuring Your Wireless Settings*** on page 17.

   To access the Internet from any computer connected to your wireless modem router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the wireless modem router's Internet LED blink, indicating communication to the ISP. If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed and no security will be implemented on the wireless modem router.

Connecting Additional Wireless Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Adding More WPS Clients

Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** check box is selected in the Advanced Wireless screen (listed under the Advanced heading in the wireless modem router main menu). If you clear this check box, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the wireless modem router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in ***Using a WPS Button to Add a WPS Client*** on page 27 or ***Using PIN Entry to Add a WPS Client*** on page 29.
2. To view a list of all devices connected to your wireless modem router (including wireless and Ethernet-connected), see ***Viewing a List of Attached Devices*** on page 59.

Adding Both WPS and Non-WPS Clients

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see ***Manually Configuring Your Wireless Security*** on page 21).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the wireless modem router:

1. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see ***Manually Configuring Your Wireless Security*** on page 21). and click **Apply**.
2. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the SSID, WPA/PSK + WPA2/PSK security method, and passphrase.
4. For the WPS devices that you want to connect, follow the procedure ***Using a WPS Button to Add a WPS Client*** on page 27 or ***Using PIN Entry to Add a WPS Client*** on page 29.

Note: To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the WPS Settings screen.

5. To view a list of all devices connected to your wireless modem router (including wireless and Ethernet-connected), see ***Viewing a List of Attached Devices*** on page 59.

Configuring Advanced WPS Settings

From the main menu, select Advanced Wireless Settings to display the following screen:

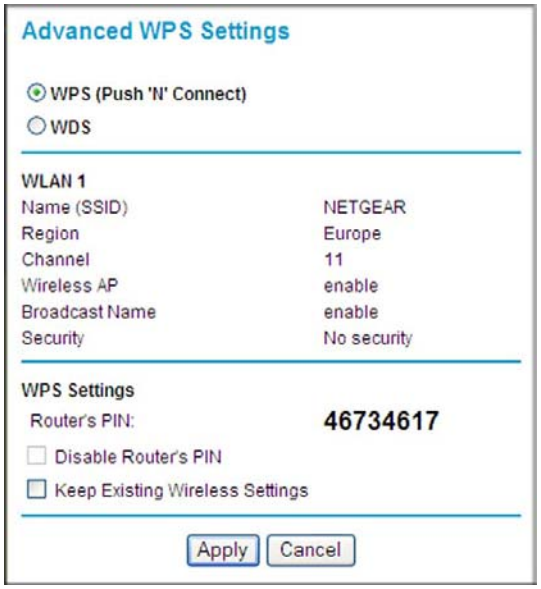


Figure 12.

The WPS settings show the wireless modem router PIN, **Disable Router's PIN**, and the **Keep Existing Wireless Settings** check box.

By default, the **Keep Existing Wireless Settings** check box is cleared. This allows the wireless modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless modem router automatically selects this check box so that your SSID and wireless security settings remain the same if you add WPS-enabled devices or if you manually add non WPS-capable devices later.

Note: If you clear the **Keep Existing Wireless Settings** check box, all wireless settings and connections will be lost if a WPS client is

added.

Protecting Your Network

3

This chapter describes how to use the basic firewall features of the wireless modem router to protect your network. This chapter includes:

- **Protecting Access to Your N300 Wireless Modem Router**
- **Viewing Logs of Web Access or Attempted Web Access**
- **Blocking Sites**
- **Firewall Rules**
- **Services**
- **Setting Times and Scheduling Firewall Services**
- **Configuring E-mail Alerts and Web Access Log Notifications**

Protecting Access to Your N300 Wireless Modem Router

For security reasons, the wireless modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the wireless modem router user name and **password** for the wireless modem router password. You can use the following procedures to change the wireless modem router's password and the period for the administrator's login time-out.

Note: The user name and password are not the same as any other user name or password your might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper case and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

How to Change the Built-In Password

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless modem router.

Figure 13.

2. In the main menu, under Maintenance, select Set Password to display the following screen:

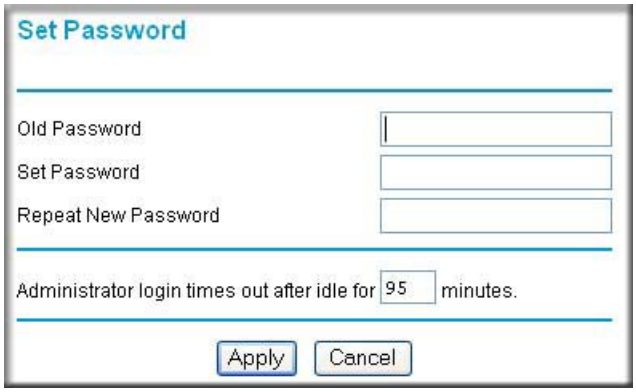


Figure 14.

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

Note: After changing the password, you are required to log in again to continue the configuration. If you have backed up the wireless modem router settings previously, you should do a new backup so that the saved settings file includes the new password.

Changing the Administrator Login Time-out

For security, the administrator's login to the wireless modem router configuration times out after a period of inactivity. To change the login time-out period:

1. In the Set Password screen, type a number in the **Administrator login times** out field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **Logs** under Security in the main menu. The Logs screen displays.

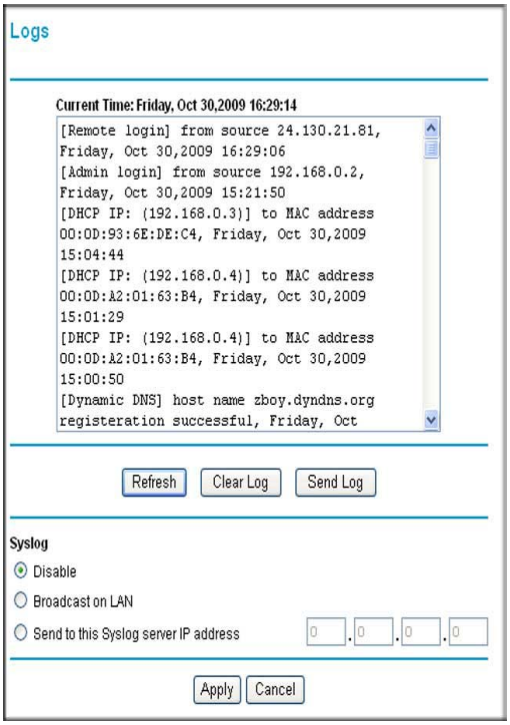

Logs
Current Time: Friday, Oct 30,2009 16:29:14
[Remote login] from source 24.130.21.81, Friday, Oct 30,2009 16:29:06
[Admin login] from source 192.168.0.2, Friday, Oct 30,2009 15:21:50
[DHCP IP: (192.168.0.3)] to MAC address 00:0D:93:6E:DE:C4, Friday, Oct 30,2009 15:04:44
[DHCP IP: (192.168.0.4)] to MAC address 00:0D:A2:01:63:B4, Friday, Oct 30,2009 15:01:29
[DHCP IP: (192.168.0.4)] to MAC address 00:0D:A2:01:63:B4, Friday, Oct 30,2009 15:00:50
[Dynamic DNS] host name zboy.dyndns.org registeration successful, Friday, Oct
Refresh
Clear Log
Send Log
Syslog
Disable
Broadcast on LAN
Send to this Syslog server IP address
0 . 0 . 0 . 0
Apply
Cancel

Figure 15.

Field	Description
Date and time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the website or newsgroup visited or to which access was attempted.
Action	Whether the access was blocked or allowed.

- To refresh the log screen, click the **Refresh** button.
- To clear the log entries, click the **Clear Log** button.
- To e-mail the log immediately, click the **Send Log** button.

Blocking Sites

The wireless modem router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the N300 Wireless Modem Router prevents objectionable content from reaching your PCs. The wireless modem router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound service blocking. Limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death, SYN flood, LAND Attack, and IP spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

The following section explains how to configure your wireless modem router to perform these functions.

To block keywords and sites:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you might have previously set for the wireless modem router.
2. In the main menu, under Security, select **Block Sites** to display the following screen

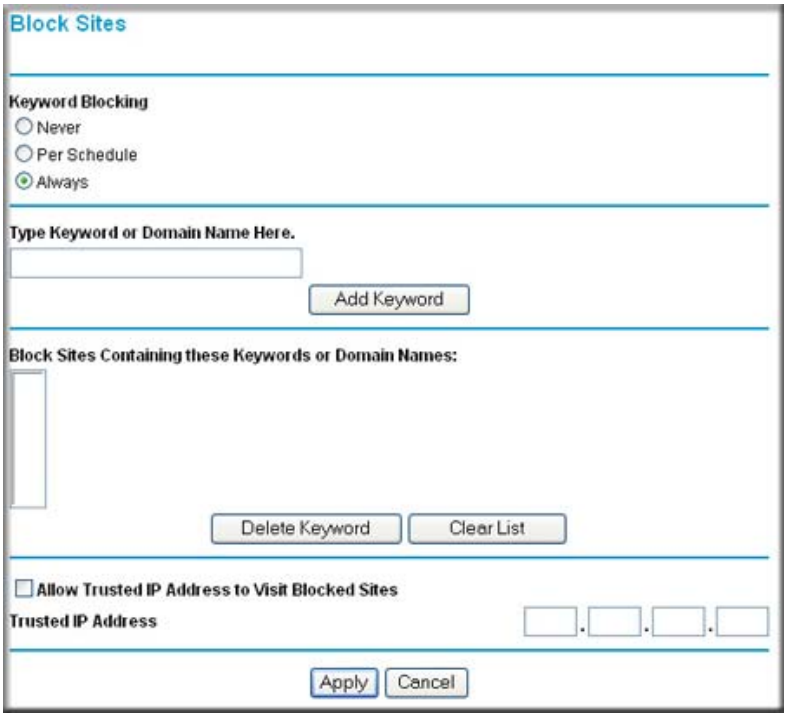


Figure 16.

3. To enable keyword blocking, select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings in the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
4. Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

   Some examples of keyword application follow:

   - If the keyword XXX is specified, the URL http://www.badstuff.com/xxx.html is blocked.
   - If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
   - Enter a period (**.**) as to block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.
5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and click **Apply**.

   You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.
7. Click **Apply** to save your settings.

Firewall Rules

Firewall rules block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the wireless modem router are:

- Inbound. Block all access from outside except responses to requests from the LAN side.
- Outbound. Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often takes effect first. See ***Order of Precedence for Rules*** on page 44 for more details.

To access the rules configuration of the wireless modem router, select **Firewall Rules** on the main menu, and then click **Add** for either an outbound or inbound service. The Firewall Rules screen displays.

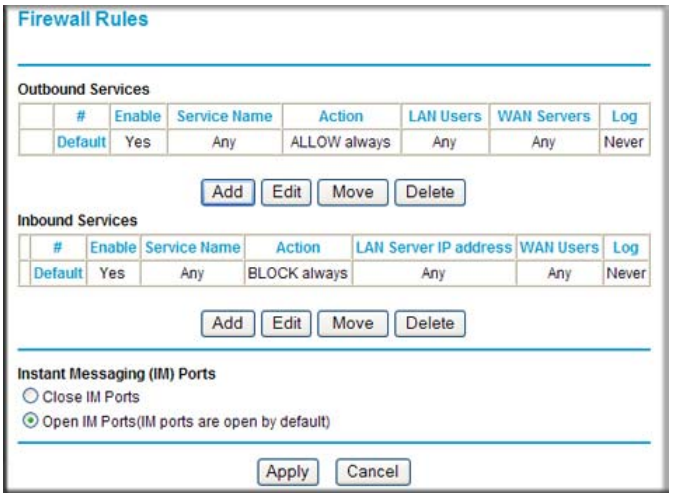

Firewall Rules
Outbound Services
Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Instant Messaging (IM) Ports
Close IM Ports
Open IM Ports(IM ports are open by default)
Apply Cancel

Figure 17.

- To edit an existing rule, select its button on the left side of the table, and click **Edit**.
- To delete an existing rule, select its button on the left side of the table, and click **Delete**.
- To move an existing rule to a different position in the table, select its button on the left side of the table, and click **Move**. At the prompt, enter the number of the desired new position and click **OK**.

Inbound Rules (Port Forwarding)

Because the wireless modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the wireless modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. Following are two application examples of inbound rules.

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in the following figure:

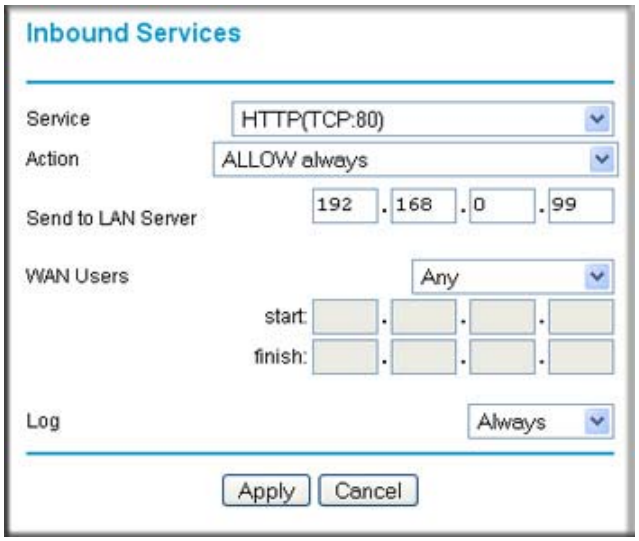


Figure 18.

The settings are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear. See ***How to Change the Built-In Password*** on page 34.
- **Action**. Choose how you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen.
- **Send to LAN Server**. Enter the IP address of the computer or server on your LAN that will receive the inbound traffic covered by this rule.
- **WAN Users**. These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the option that you want:
  - **Any**: All IP addresses are covered by this rule.
  - **Address range**: If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**: Enter the required address in the **Start** field.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the settings and action will be logged.
  - **Not match**. Traffic of this type that does not match the settings and action will be logged.

Inbound Rule Example: Allowing Video Conferencing

If you want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in the following figure, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed settings.

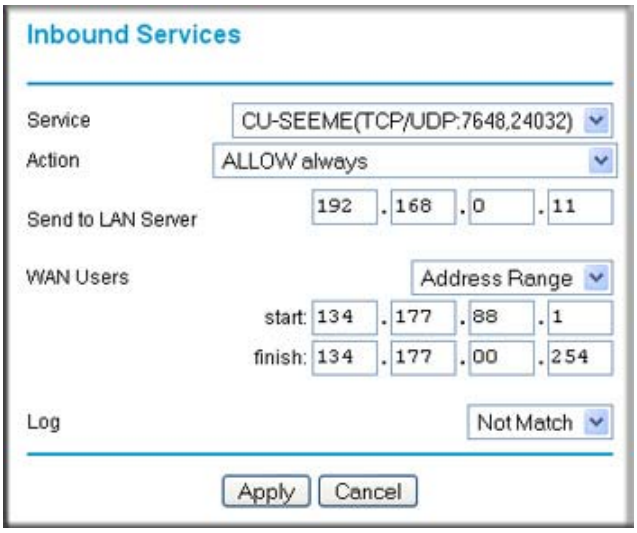


Figure 19.

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP Setup screen to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example in the previous figure). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The wireless modem router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on the following:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

The following is an application example of outbound rules.

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you create in the Schedule screen.You can specify that the wireless modem router logs any attempt to use Instant Messenger during this blocked period. You can also open or close AOL or MSN Instant Messenger ports: see the Firewall Rules screen in the ***Order of Precedence for Rules*** on page 44.

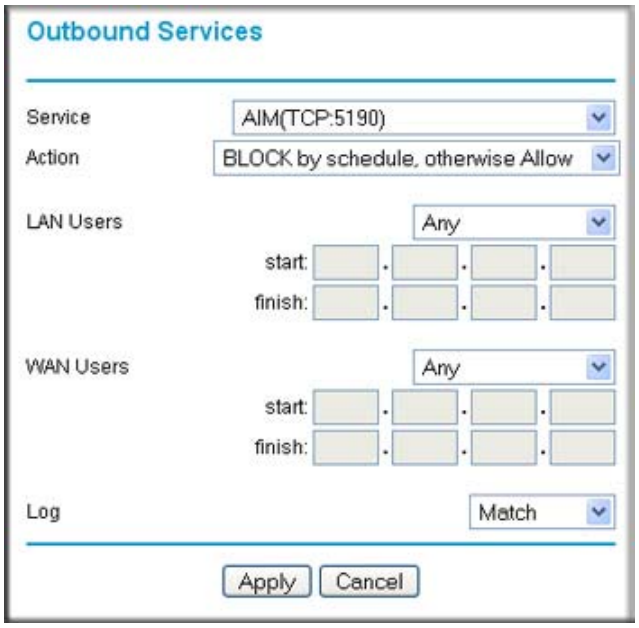


Figure 20.

The settings are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the **Add Custom Service** button in the Services screen to add any additional services or applications that do not already appear.
- **Action**. Choose how you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen.
- **LAN Users**. These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.
- **WAN Users**. These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.

  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the settings and action will be logged.
  - **Not match**. Traffic of this type that does not match the settings and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Firewall Rules screen, as shown in the following figure:

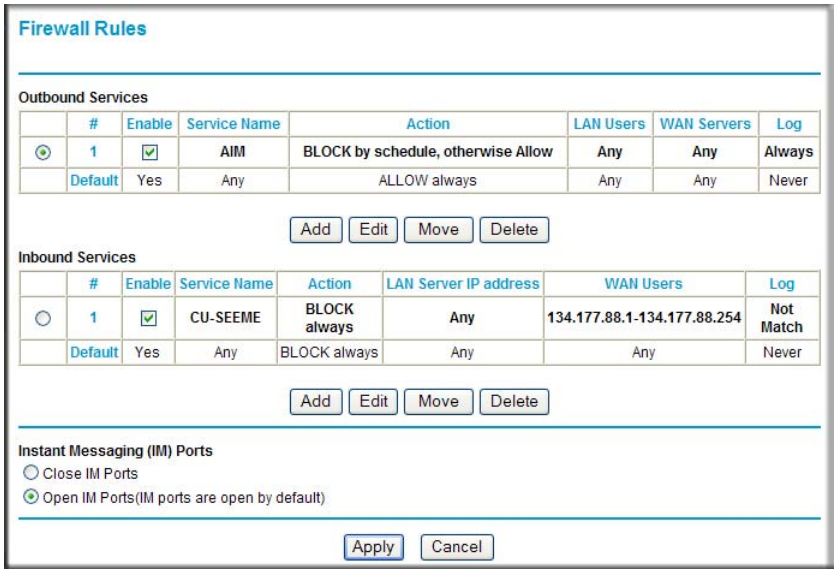

Firewall Rules
Outbound Services
Enable Service Name Action LAN Users WAN Servers Log
1 AIM BLOCK by schedule, otherwise Allow Any Any Always
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
Enable Service Name Action LAN Server IP address WAN Users Log
1 CU-SEEME BLOCK always Any 134.177.88.1-134.177.88.254 Not Match
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Instant Messaging (IM) Ports
Close IM Ports
Open IM Ports(IM ports are open by default)
Apply Cancel

Figure 21.

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. The **Move** button allows you to relocate a defined rule to a new position in the table.

The Firewall Rules screen also lets you open or close AOL or MSN Instant Messenger ports:

1. Under Instant Messaging (IM) Ports, select a radio button:
   - **Close IM Ports**. Specifies to disable instant messaging traffic.
   - **Open IM Ports**. Specifies to enable instant messaging traffic. IM ports are open by default.
2. Click **Apply** to save your changes.

Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the wireless modem router already holds a list of many service port numbers, you are not limited to these choices. Use the following procedure to create your own service definitions.

To add or change a service:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the wireless modem router.
2. Below the Security heading, select Services to display the Services screen shown in the following figure:

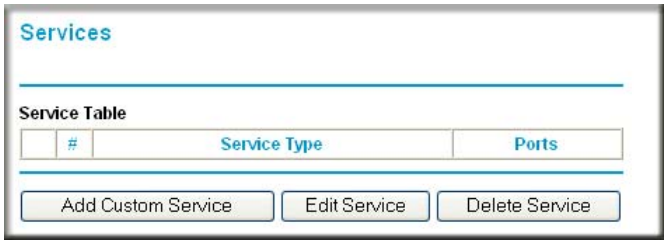


Figure 22.

- To create a new service, click the **Add Custom Service** button.
- To edit an existing service, select its button on the left side of the table, and click **Edit Service**.
- To delete an existing service, select its button on the left side of the table, and click **Delete Service**.

3. Use the **Add Services** screen to define or edit a service.

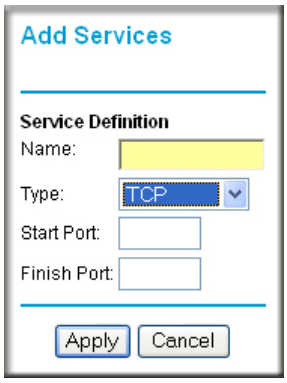


Figure 23.

4. Click **Apply** to save your changes.

Setting Times and Scheduling Firewall Services

The wireless modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

Setting Your Time Zone

To localize the time for your log entries, you must specify your time zone:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless modem router.
2. Select Schedule below Security to display the Schedule screen.

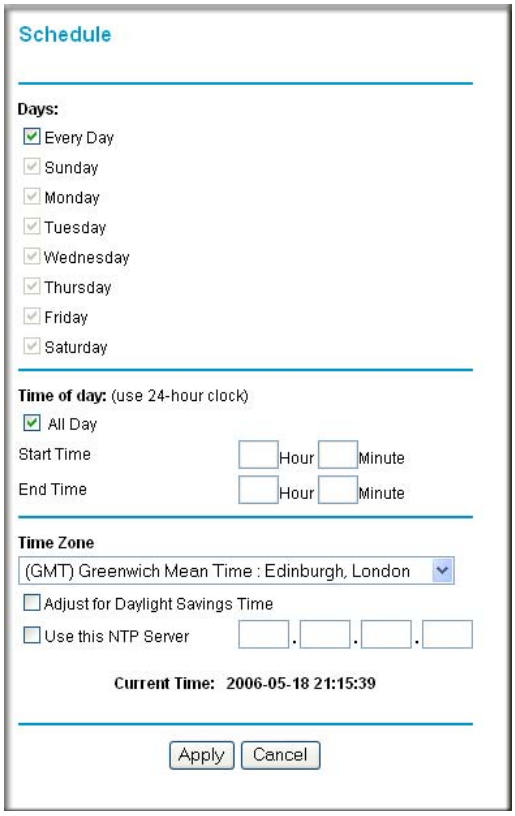


Figure 24.

3. Select your time zone. This setting is used for the blocking schedule according to your local time zone and for time-stamping log entries.

   Select the **Adjust for Daylight Savings Time** check box if your time zone is currently in daylight savings time.

Note: If your region uses daylight savings time, you must manually select Adjust for Daylight Savings Time on the first day of daylight savings

time, and clear it at the end. Enabling daylight savings time causes one hour to be added to the standard time.

4. The wireless modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.
5. Click **Apply** to save your settings.

Scheduling Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless modem router.
2. Select Schedule below Security to display the Schedule screen that is shown in **Figure 24**.
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, or enter times in the **Start Time** and **End Time** fields.

Note: Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.

4. Click **Apply** to save your changes.

Configuring E-mail Alerts and Web Access Log Notifications

To receive logs and alerts by e-mail, you must provide your e-mail account information.

To configure e-mail alert and web access log notifications:

1. Select E-mail under Security in the main menu. The E-mail screen displays.

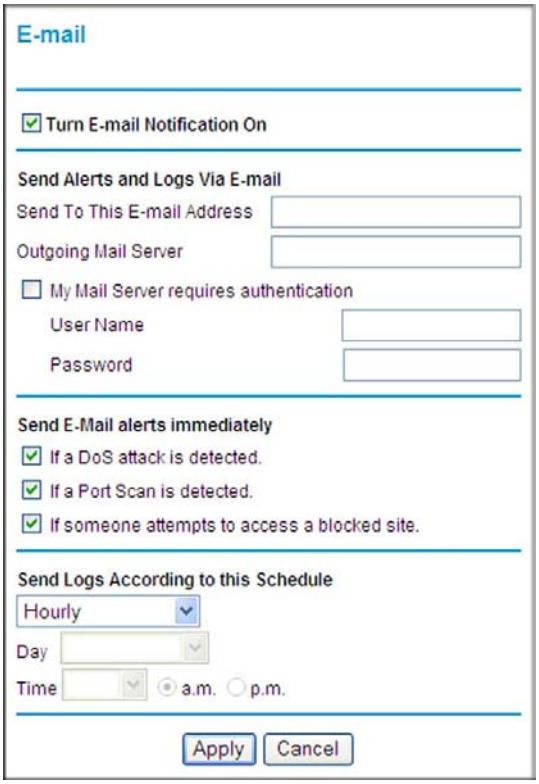


Figure 25.

2. Select the **Turn E-mail Notification On** check box.
3. Enter your email details:
   - Enter the name of your ISP's outgoing (SMTP) mail server (such as **mail.myISP.com**) in the **Your Outgoing Mail Server** field. You might be able to find this information in the configuration screen of your e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail.
   - Enter the e-mail address to which logs and alerts are sent in the **Send To This E-mail Address** field. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by e-mail.
   - If your outgoing e-mail server requires authentication, select the **My Mail Server requires authentication** check box.
     - Enter your user name for the outgoing e-mail server in the **User Name** field.
     - Enter your password for the outgoing e-mail server in the **Password** field.

4. You can specify that logs are automatically sent by e-mail with these options:
   - **Send alert immediately**. Select this check box for immediate notification of attempted access to a blocked site or service.
   - **Send Logs According to this Schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
     - **Day**. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
     - **Time**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the Wireless Modem Router's memory. If the Wireless Modem Router cannot e-mail the log file, the log buffer might fill up. In this case, the wireless modem router overwrites the log and discards its contents.
5. Click **Apply** to save your settings.

   So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Managing Your Network

4

This chapter describes features to help you manage your N300 Wireless Modem Router. This chapter includes the following sections:

- **Upgrading the Firmware**
- **Viewing N300 Wireless Modem Router Status Information**
- **Viewing a List of Attached Devices**
- **Managing the Configuration File**
- **Running Diagnostic Utilities and Rebooting the N300 Wireless Modem Router**
- **Enabling Remote Management Access**

Note: For help with changing the password, see ***How to Change the Built-In Password*** on page 34.

Upgrading the Firmware

The wireless modem router's firmware (routing software) is stored in flash memory. By default, when you log in to your wireless modem router, it automatically checks the NETGEAR website for new firmware and alerts you if there is a newer version.

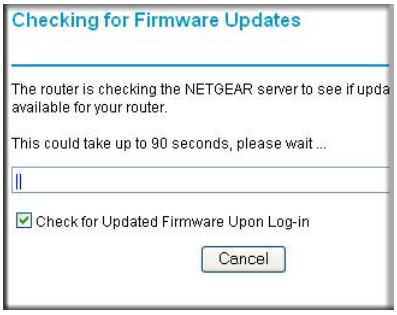

Checking for Firmware Updates
The router is checking the NETGEAR server to see if upda
available for your router.
This could take up to 90 seconds, please wait ...
Check for Updated Firmware Upon Log-in
Cancel

Figure 26.

Note: To turn off the automatic firmware check at log in, clear the **Check for Updated Firmware Upon Log-in** check box on the Router Upgrade screen.

If the wireless modem router discovers a newer version of firmware, the message on the left displays. If no new firmware is available, the message on the right displays.

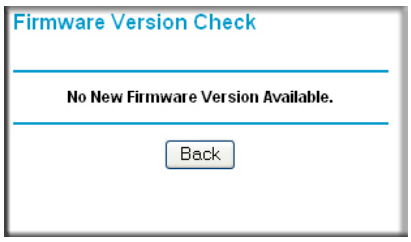


Figure 27.

To upgrade, click **Yes** to allow the wireless modem router to download and install the new firmware

WARNING!

When uploading firmware to the wireless modem router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware..

When the upload is complete, your wireless modem router automatically restarts. The upgrade process could take a few minutes. Read the new firmware release notes to determine whether you must reconfigure the Wireless Modem Router after upgrading.

Manually Checking for Firmware Upgrades

You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

To manually check for new firmware and install it on your wireless modem router:

1. Under Maintenance on the main menu, select Router Status. Note the version number of your wireless modem router firmware.
2. Go to the DGN3500 support page on the NETGEAR website at *http://www.netgear.com/support*.
3. If the firmware version on the NETGEAR website is newer than the firmware on your wireless modem router, download the file to your computer.
4. Under Maintenance on the wireless modem router main menu, select Router Upgrade to display the following screen:

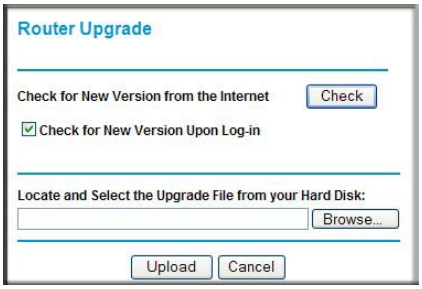


Figure 28.

5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img or .chk).
6. Click **Upload** to send the firmware to the wireless modem router

WARNING!

When uploading firmware to the wireless modem router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your Wireless Modem Router automatically restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to determine whether you must reconfigure the Wireless Modem Router after upgrading.

Viewing N300 Wireless Modem Router Status Information

To view wireless modem router status and usage information, from the main menu, under the Maintenance heading, select Router Status. The Router Status screen displays.

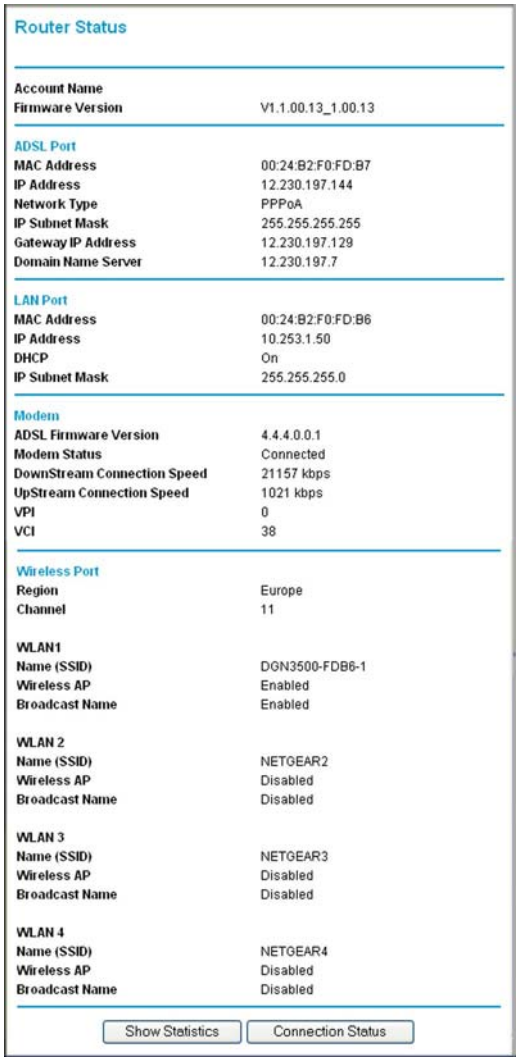


Figure 29.

You can use the Show Statics and Connection Status buttons to view additional status information, as described in ***Connection Status*** on page 57 and ***Statistics*** on page 58. The following table explains Router Status screen fields.

Field	Description
Account Name	The host name assigned to the wireless modem router.
Firmware Version	The version of the wireless modem router firmware. It changes if you upgrade the wireless modem router.

Field		Description
ADSL Port	MAC Address	This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the wireless modem router.
	IP Address	This field displays the IP address being used by the Internet (ADSL) port of the wireless modem router. If no address is shown, the wireless modem router cannot connect to the Internet.
	Network Type	The network type depends upon your ISP.
	IP Subnet Mask	This field displays the IP subnet mask being used by the Internet (ADSL) port of the wireless modem router.
	Gateway IP Address	IP address used as a gateway to the Internet for computers configured to use DHCP.
	Domain Name Server	This field displays the DNS server IP addresses being used by the wireless modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the wireless modem router.
	IP Address	The IP address being used by the Ethernet (LAN) port of the wireless modem router. The default is 192.168.0.1.
	DHCP	Identifies whether the firmware's built-in DHCP server is active for the LAN-attached devices.
	IP Subnet Mask	The IP subnet mask being used by the Ethernet (LAN) port of the wireless modem router. The default is 255.255.255.0.
Modem	ADSL Firmware Version	The version of the firmware.
	Modem Status	The connection status of the modem.
	DownStream Connection Speed	The connection speed of the ADSL connection from the phone company to your wireless modem router
	UpSTream Connection Speed	The connection speed of the ADSL connection from your wireless modem router to the phone company
	VPI	The VPI settings from the ADSL Settings screen.
	VCI	The VCI settings from the ADSL Settings screen.
Wireless Port	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is enabled for WLAN1. If disabled, the Wireless LED on the front panel is off.

Field		Description
WLAN1 WLAN2 WLAN3 WLAN4	Name (SSID)	The wireless network name.
	Wireless AP	Indicates if the access point feature is enabled.
	Broadcast Name	Indicates if the wireless modem router is configured to broadcast its SSID for WLAN2.

Connection Status

To view the connection status, on the Router Status screen, click **Connection Status**.

Figure 30.

- Click the **Connect** button, and the wireless modem router attempts to connect to the Internet.
- Click the **Disconnect** button to disconnect the wireless modem router Internet connection.
- Click the **Close Window** button to close the Connection Status screen.

The following table describes the connection status settings.

Item	Description
Connection Time	The time elapsed since the last connection to the Internet through the ADSL port.
Connecting to sender	The connection status.
Negotiation	Success or Failed.
Authentication	Success or Failed.
Obtaining IP Address	The IP address assigned to the WAN port by the ADSL Internet Service Provider.
Obtaining Network Mask	The network mask assigned to the WAN port by the ADSL Internet Service Provider.

Statistics

To view statistics, on the Router Status screen, click **Show Statistics**.

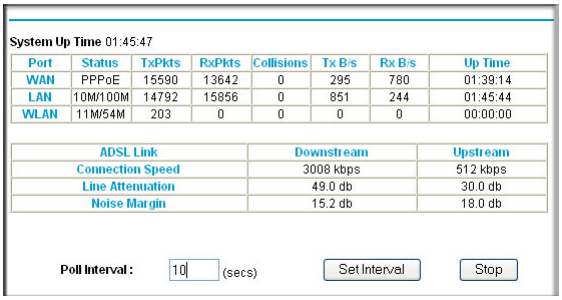

System Up Time 01:45:47
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN PPPoE 15590 13642 0 295 780 01:39:14
LAN 10M/100M 14792 15856 0 851 244 01:45:44
WLAN 11M/54M 203 0 0 0 0 00:00:00
ADSL Link Downstream Upstream
Connection Speed 3008 kbps 512 kbps
Line Attenuation 49.0 db 30.0 db
Noise Margin 15.2 db 18.0 db
Poll Interval : 10 (secs) Set Interval Stop

Figure 31.

The following table describes the wireless modem router statistics.

Item		Description
System Up Time		The time elapsed since the wireless modem router was last restarted.
Port		The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:
	Status	The link status of the port.
	TxPkts	The number of packets transmitted on this port since reset or manual clear.
	RxPkts	The number of packets received on this port since reset or manual clear.
	Collisions	The number of collisions on this port since reset or manual clear.
	Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
	Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
	Up Time	The time elapsed since this port acquired the link.
Poll Interval		The intervals at which the statistics are updated in this screen.

- To change the polling frequency, enter a time in seconds in the **Poll Interval** field, and click **Set Interval**.
- To stop the polling, click **Stop**.

Viewing a List of Attached Devices

The Attached Devices table lists all IP devices that the wireless modem router has discovered on the local network. From the main menu, under Maintenance, select **Attached Devices** to view the table.

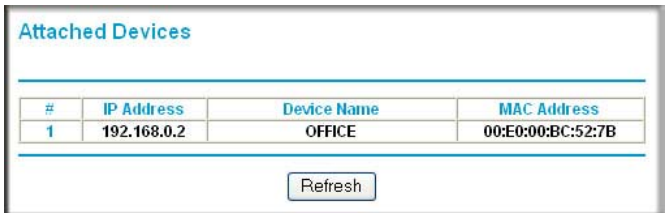


Figure 32.

For each device, the table shows the IP address, NetBIOS host name or device name (if available), and the Ethernet MAC address. To force the wireless modem router to look for attached devices, click **Refresh**.

Note: If the Wireless Modem Router is rebooted, the table data is lost until the wireless modem router rediscovers the devices.

Managing the Configuration File

The configuration settings of the N300 Wireless Modem Router are stored within the wireless modem router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings. From the main menu, under Maintenance, select Backup Settings.

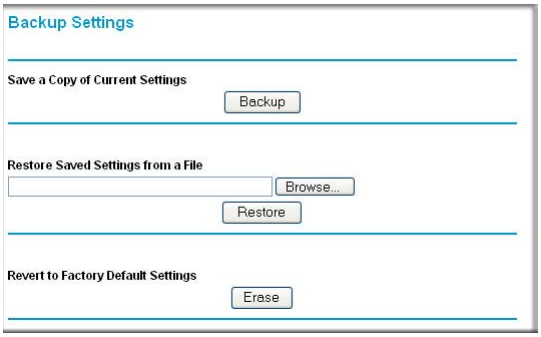


Figure 33.

The following sections describe the available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Backup Settings screen let you save and retrieve a file containing your Wireless Modem Router's configuration settings.

To save your settings, click **Back Up**. Your browser extracts the configuration file from the Wireless Modem Router and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as comcast.cfg.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

To restore your settings from a saved configuration file, enter the full path to the file on your computer, or click **Browse** to browse to the file. When you have located it, click **Restore** to send the file to the wireless modem router. The wireless modem router then reboots automatically.

WARNING!

Do not interrupt the reboot process.

Erasing the Configuration

Under some circumstances (for example, if you move the wireless modem router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings. After an erase, the wireless modem router's user name is **admin**, the password is **password**, the LAN IP address is **192.168.0.1**, and its DHCP server is enabled.

- To erase the configuration, click the **Erase** button in the Backup Settings screen.
- To restore the factory default configuration settings when you do not know the login password or IP address, you must use the restore factory settings button on the rear panel of the wireless modem router (see *Factory Default Configuration* on page 115).

Running Diagnostic Utilities and Rebooting the N300 Wireless Modem Router

The wireless modem router has a diagnostics feature. In the main menu, under Maintenance, select Diagnostics to display the following screen.

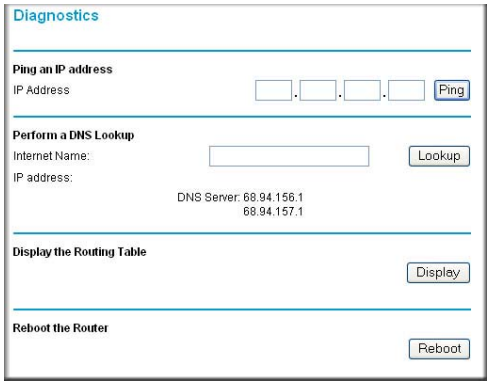


Figure 34.

You can use the Diagnostics screen to perform the following functions from the wireless modem router:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other wireless modem routers the wireless modem router is communicating with.
- Reboot the wireless modem router to enable new network configurations to take effect or to clear problems with the wireless modem router's network connection.

Enabling Remote Management Access

The remote management feature allows you to upgrade or check the status of your N300 Wireless Modem Router via the Internet. From the main menu, under Advanced, select Remote Management.

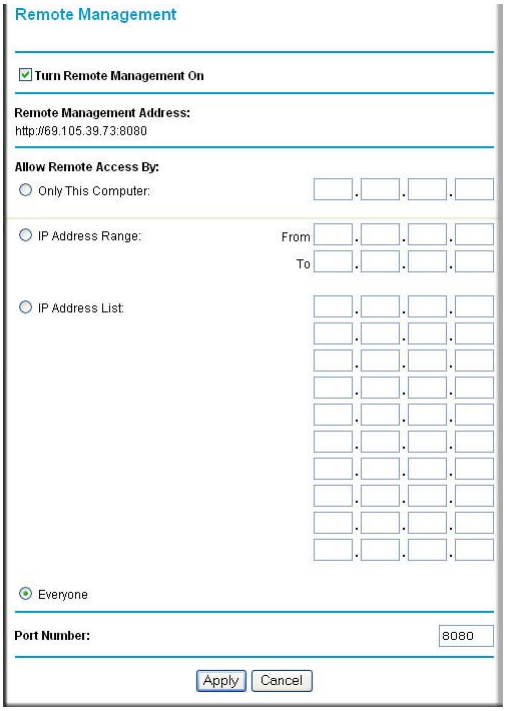


Figure 35.

Note: Be sure to change the wireless modem router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

To configure your wireless modem router for remote management:

1. Select the **Turn Remote Management On** check box.
2. Under Allow Remote Access By, specify what external IP addresses will be allowed to access the wireless modem router's remote management.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from any IP address on the Internet, select **Everyone**.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**.
  Enter a beginning and ending IP address to define the allowed range.
- To allow access from a single IP address on the Internet, select **Only This Computer**.
  Enter the IP address that will be allowed access.

3. Specify the port number for accessing the management interface.

   Normal Web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click **Apply** to have your changes take effect.

Note: When accessing your wireless modem router from the Internet, type your wireless modem router's WAN IP address into your browser's address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter **http://134.177.0.123:8080** in your browser.

Advanced Configuration

5

The wireless modem router provides a variety of advanced features, which are described in the following sections:

- **WAN Setup**
- **Configuring LAN Setup**
- **Dynamic DNS Service**
- **Setting up Static Routes**
- **Configuring Universal Plug and Play**
- **Building Wireless Bridging and Repeating Networks**

WAN Setup

To view or change the WAN settings:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the wireless modem router.
2. In the main menu, under Advanced, click WAN Setup to display the following screen.

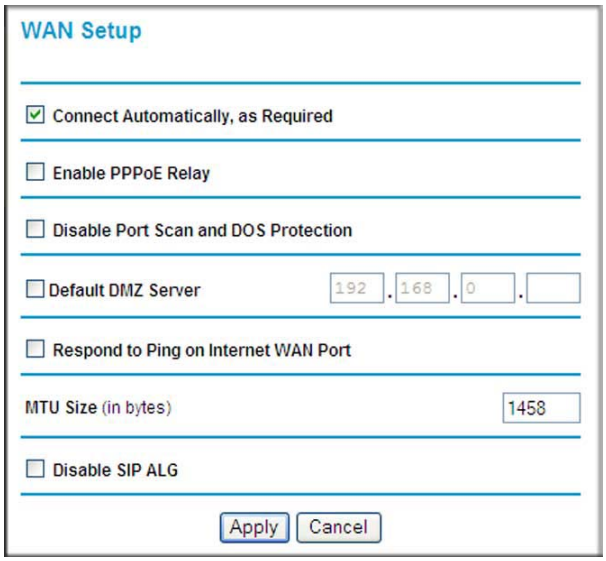


Figure 36.

The WAN Setup fields are described in the following table:

Setting	Description
Connect Automatically, as Required	Usually, this check box is selected, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can clear the check box to disable this feature. If this setting is disabled, you must connect manually, using the screen that you access by clicking the **Connection Status** button on the Status screen. If you have an Always on connection, this setting has no effect.
Enable PPPoE Relay	Selecting this check box allows a PPPoE client on a local PC to connect to a remote PPPoE server with the wireless modem router acting as a relay agent.
Disable Port Scan and DOS Protection	The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and video confrencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, ***Setting up Static Routes*** on page 78.

Setting	Description
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
Disable SIP ALG	The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The **Disable SIP ALG** check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

Setting Up a Default DMZ Server

The default demilitarized zone (DMZ) server feature is helpful when you use some online games and video confrencing applications that are incompatible with NAT. The wireless modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

Note: For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the wireless modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

To assign a computer or server to be a default DMZ server:

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the wireless modem router.
2. In the main menu, under Advanced, click WAN Setup to display the following screen.
3. On the WAN Setup screen, select the **Default DMZ Server** check box.
4. Type the IP address for that server.
5. Click **Apply** to save your changes.

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The wireless modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless modem router's default LAN IP configuration is:

- LAN IP address: **192.168.0.1**
- Subnet mask: **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

To configure LAN settings, log in to the wireless modem router, and under the Advanced heading, select LAN Setup. The following screen displays:

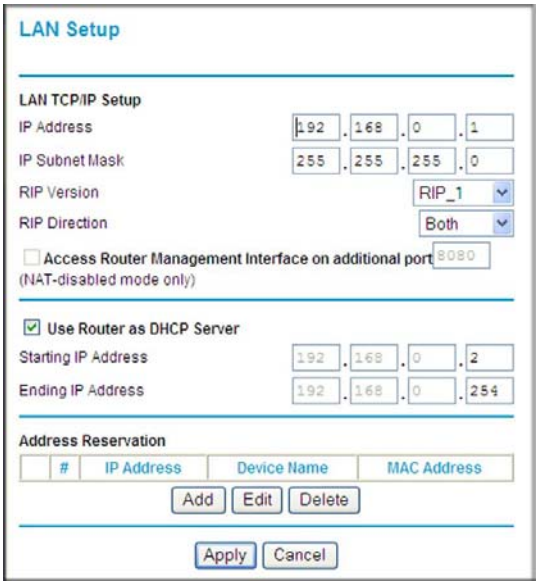


Figure 37.

If you make changes you must click **Apply** in order for the changes to take effect.

Note: If you change the LAN IP address of the wireless modem router while connected through your Internet browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

The LAN Setup fields are explained in the following table.

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the wireless modem router.
	IP Subnet Mask	The LAN subnet mask of the wireless modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or wireless modem router.
	RIP Direction	RIP (Router Information Protocol) allows a wireless modem router to exchange routing information with other routers. This setting controls how the wireless modem router sends and receives RIP packets. **Both** is the default. • **Both** or **Out Only**. The wireless modem router broadcasts its routing table periodically. • **Both** or **In Only**. The wireless modem router incorporates the RIP information that it receives. • **None**. The wireless modem router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the wireless modem router sends. It recognizes both formats when receiving. By default, this is **RIP-1**. • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information	Use Router as a DHCP Server	This check box is usually selected so that the wireless modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. See ***Using the N300 Wireless Modem Router as a DHCP Server*** on page 73.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the wireless modem router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the wireless modem router.
Address Reservation For more information, see ***Address Reservation*** on page 70.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the wireless modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Using the N300 Wireless Modem Router as a DHCP Server

By default, the wireless modem router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless modem router's LAN. The assigned default gateway address is the LAN address of the wireless modem router. The wireless modem router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the wireless modem router are satisfactory. Click the link to the online document ***Related Documents*** in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless modem router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might wish to save part of the range for devices with fixed addresses.

The wireless modem router delivers the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the wireless modem router's LAN IP address)
- Primary DNS Server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the wireless modem router's LAN IP address)
- Secondary DNS Server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you will need to set your computers' IP addresses manually or they will not be able to access the wireless modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the wireless modem router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

1. Click **Add**.
2. In the **IP Address** field, type the IP address to assign to the computer or server. (Choose an IP address from the wireless modem router's LAN subnet, such as **192.168.0.x**.)

3. Type the MAC address of the computer or server.

   Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address is not assigned until the next time the computer contacts the wireless modem router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Select the radio button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

Configuring LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The wireless modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless modem router's default LAN IP configuration is:

- LAN IP address: **192.168.0.1**
- Subnet mask: **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

To configure LAN settings, log in to the wireless modem router, and under the Advanced heading, select LAN Setup. The following screen displays:

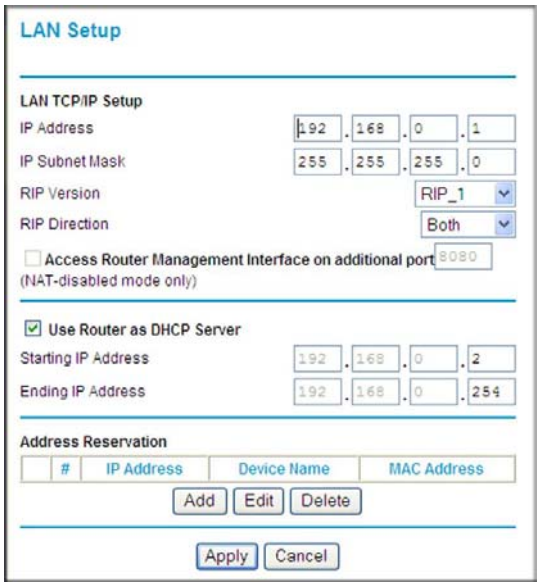


Figure 38.

If you make changes you must click **Apply** in order for the changes to take effect.

Note: If you change the LAN IP address of the wireless modem router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

The LAN Setup fields are explained in the following table.

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the wireless modem router.
	IP Subnet Mask	The LAN subnet mask of the wireless modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or wireless modem router.
	RIP Direction	RIP (Router Information Protocol) allows a wireless modem router to exchange routing information with other routers. This setting controls how the wireless modem router sends and receives RIP packets. **Both** is the default. • **Both** or **Out Only**. The wireless modem router broadcasts its routing table periodically. • **Both** or **In Only**. The wireless modem router incorporates the RIP information that it receives. • **None**. The wireless modem router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the wireless modem router sends. It recognizes both formats when receiving. By default, this is **RIP-1**. • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information	Use Router as a DHCP Server	This check box is usually selected so that the wireless modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. See ***Using the N300 Wireless Modem Router as a DHCP Server*** on page 70.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the wireless modem router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the wireless modem router.
Address Reservation For more information, see ***Address Reservation*** on page 70.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the wireless modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Using the N300 Wireless Modem Router as a DHCP Server

By default, the wireless modem router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless modem router's LAN. The assigned default gateway address is the LAN address of the wireless modem router. The wireless modem router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the wireless modem router are satisfactory. Click the link to the online document ***Related Documents*** in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless modem router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might wish to save part of the range for devices with fixed addresses.

The wireless modem router delivers the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the wireless modem router's LAN IP address)
- Primary DNS Server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the wireless modem router's LAN IP address)
- Secondary DNS Server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you will need to set your computers' IP addresses manually or they will not be able to access the wireless modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the wireless modem router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

1. Click **Add**.
2. In the **IP Address** field, type the IP address to assign to the computer or server. (Choose an IP address from the wireless modem router's LAN subnet, such as **192.168.0.x**.)

3. Type the MAC address of the computer or server.

   Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address is not assigned until the next time the computer contacts the wireless modem router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Select the radio button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

Dynamic DNS Service

If your Internet Service Provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service, which allows you to register your domain to their IP address, and forwards traffic directed at your domain to your frequently changing IP address.

Note: If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service will not work because private addresses are not routed on the Internet.

Your wireless modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. You must first visit their website at *www.dyndns.org* and obtain an account and host name, which you configure in the wireless modem router. Then, whenever your ISP-assigned IP address changes, your wireless modem router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your wireless modem router at hostname.dyndns.org.

From the main menu, under Advanced, select Dynamic DNS to display the Dynamic DNS screen.

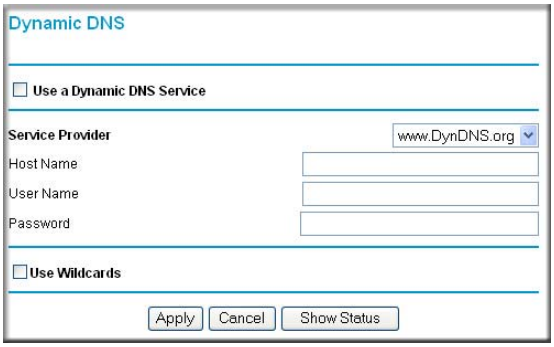


Figure 39.

To configure Dynamic DNS:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the **Service Provider** list. For example, for DynDNS.org, select **www.dyndns.org**.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your Dynamic DNS service provider.

4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Setting up Static Routes

Static routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the wireless modem router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route setup would look like **Figure 41**.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- The value in the **Metric** field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Configuring Static Routes

1. Log in to the wireless modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the wireless modem router.

2. In the main menu, under Advanced, select **Static Routes** to display the Static Routes table.

Figure 40.

3. To add a static route:
   a. Click **Add** to open the following Static Routes screen.

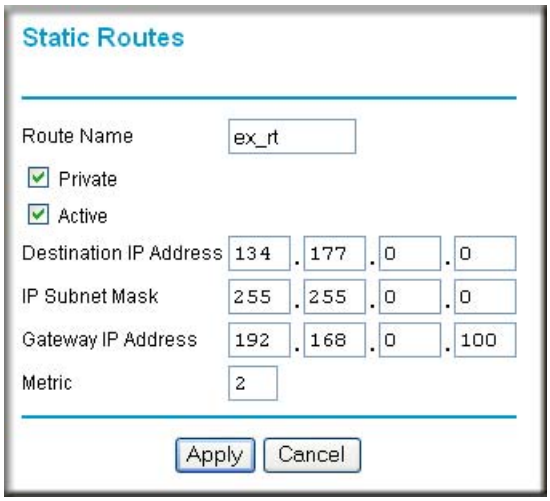

Static Routes
Route Name ex_rt
Private
Active
Destination IP Address 134 . 177 . 0 . 0
IP Subnet Mask 255 . 255 . 0 . 0
Gateway IP Address 192 . 168 . 0 . 100
Metric 2
Apply Cancel

Figure 41.

   b. Enter a route name for this static route in the **Route Name** field. This name is for identification purpose only.
   c. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
   d. Select **Active** to make this route effective.
   e. Enter the destination IP address of the final destination.
   f. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.
   g. Enter the gateway IP address, which must be a router on the same LAN segment as the router.
   h. Enter a number between 2 and 15 as the metric value in the **Metric** field. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.
4. Click **Apply**. The Static Routes table is updated to show the new entry.

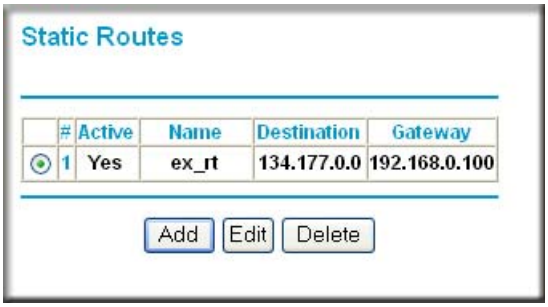

Static Routes
Active Name Destination Gateway
1 Yes ex_rt 134.177.0.0 192.168.0.100
Add Edit Delete

Figure 42.

Configuring Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Select UPnP on the main menu to display the UPnP screen:

Figure 43.

2. Fill in the settings on the UPnP screen:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the wireless modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless modem router.
   - **Advertisement Period**. The advertisement period is how often the wireless modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the wireless modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.
3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the wireless modem router.
   - Click **Cancel** to disregard any unsaved changes.

- Click Refresh to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Building Wireless Bridging and Repeating Networks

With the wireless modem router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the modem router with other access points (APs) and wireless devices, you can connect clients by using their MAC addresses rather than by specifying IP addresses.

Here are some examples of wireless bridged configurations:

- **Point-to-point bridge**. The wireless modem router communicates with another bridge-mode wireless station. See **Configuring a Point-to-Point Bridge Configuration**."
- **Multi-point bridge**. The wireless modem router is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See **Configuring a Repeater with Wireless Client Association**."
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See **Configuring a Repeater with Wireless Client Association**."

Note: The wireless bridging and repeating feature uses the default security profile to send and receive traffic.

To view or change these configurations, select Advanced Wireless Settings from the main menu, and then select the **WDS** radio button:

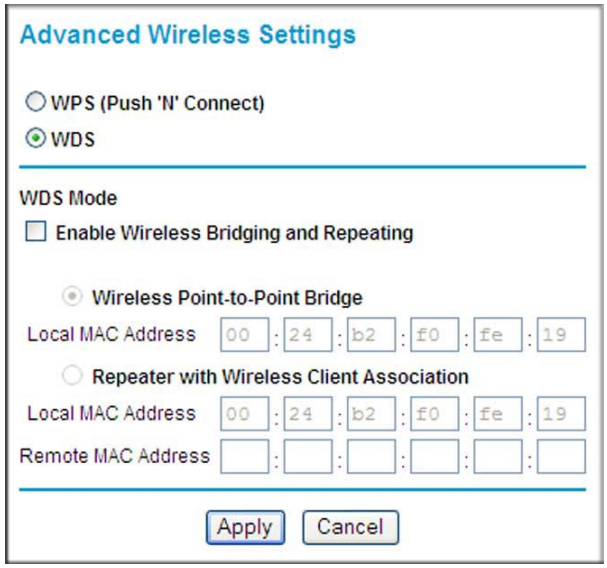

Advanced Wireless Settings
WPS (Push 'N' Connect)
WDS
WDS Mode
Enable Wireless Bridging and Repeating
Wireless Point-to-Point Bridge
Local MAC Address 00 : 24 : b2 : f0 : fe : 19
Repeater with Wireless Client Association
Local MAC Address 00 : 24 : b2 : f0 : fe : 19
Remote MAC Address
Apply
Cancel

Figure 44.

Configuring a Point-to-Point Bridge Configuration

In point-to-point bridge mode, the wireless modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled—only wired clients can be connected. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication.

The following figure shows an example of point-to-point bridge mode.

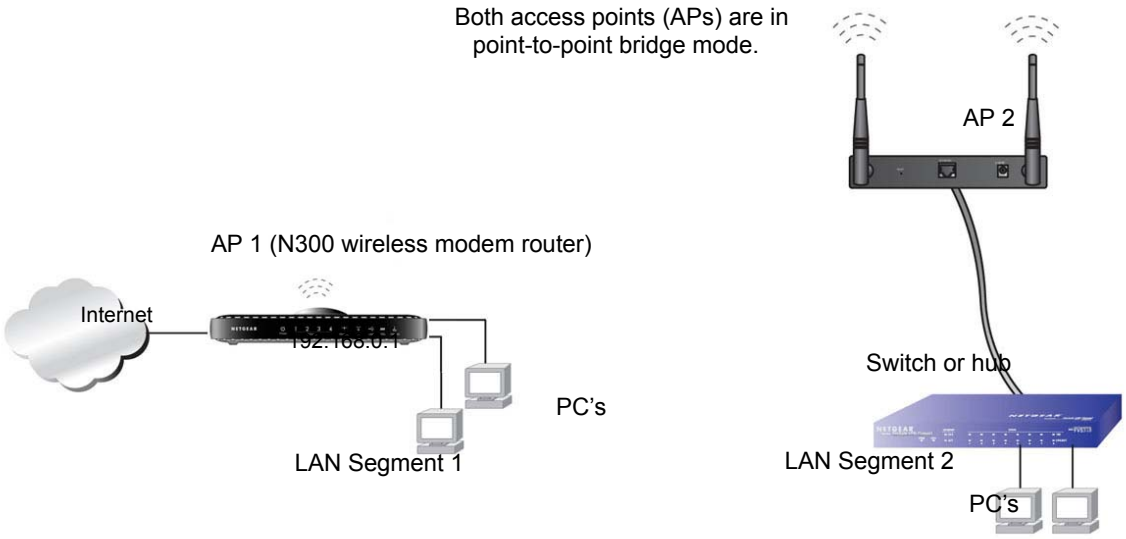


Figure 45.

To set up a point-to-point bridge configuration (shown in Figure 45):

1. Configure the wireless modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.
2. Configure the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

   The wireless modem router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the MAC address in its **Remote MAC Address** field.
3. Configure both APs and verify that both APs are using the same SSID, channel, authentication mode, if any, and security settings if security is in use.
4. Disable the DHCP server on AP2. AP1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Configuring a Repeater with Wireless Client Association

In the repeater mode with wireless client association, the wireless modem router sends all traffic to a remote AP. For the repeater mode, you must enter the MAC address of the remote "parent" access point. Alternatively, you can configure the wireless modem router as the parent by entering the address of a "child" access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this wireless modem router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the wireless modem router is the parent AP, it can connect with up to four child APs.

The following figure shows an example of a Repeater mode configuration.

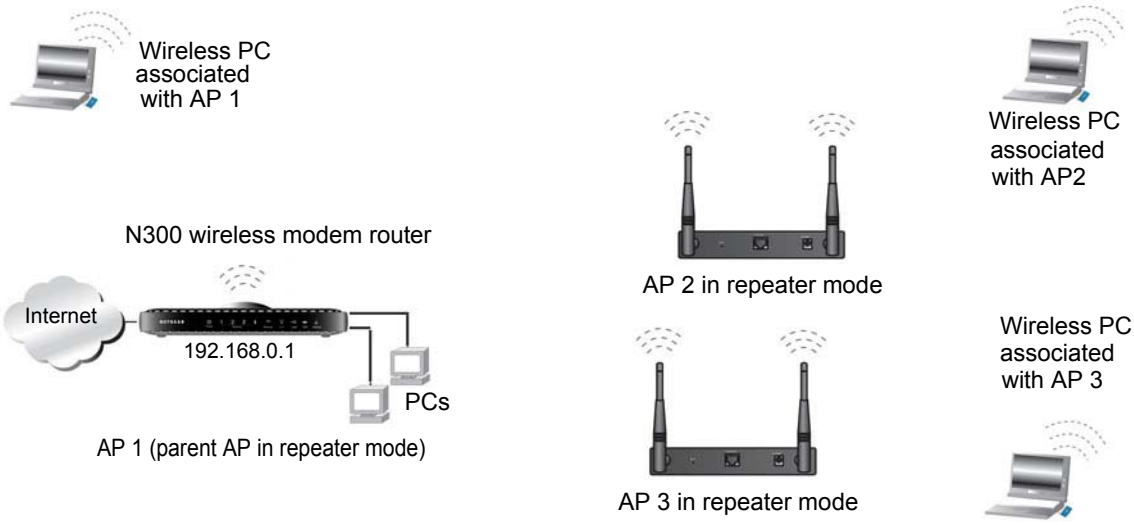


Figure 46.

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
   - Configure AP 1 (the wireless modem router in **Figure 46**) on with the MAC address of AP 2 and AP 3 in the first two **Remote MAC Address** fields.
   - Configure AP 2 with the MAC address of AP 1 in the **Remote MAC Address** field.
   - Configure AP 3 with the MAC address of AP 1 in the **Remote MAC Address** field.
2. Verify the following for both access points:
   - The LAN network configuration of each AP is configured to operate in the same LAN network address range as the LAN devices.
   - The APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same network.

- If you are using DHCP, AP devices should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.
- AP devices must use the same SSID, channel, authentication mode, and encryption.

3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

USB Storage

6

This chapter describes how to access and configure a USB storage drive attached to your wireless modem router.

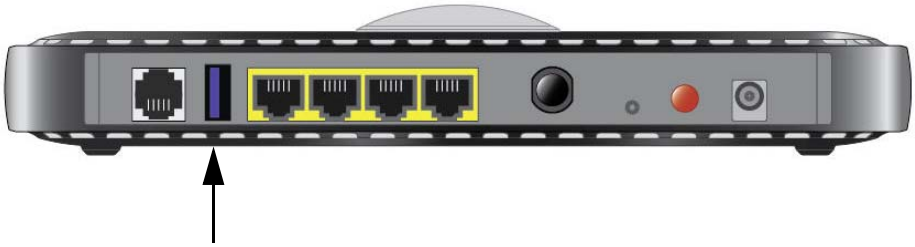


Figure 47.

Note: The USB port on the wireless modem router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the wireless modem router USB port.

This chapter includes the following sections:

- **USB Drive Requirements**
- **File Sharing Scenarios**
- **USB Storage Basic Settings**
- **Editing a Network Folder**
- **Configuring USB Storage Advanced Settings**
- **Unmounting a USB Drive**
- **Specifying Approved USB Devices**
- **Connecting to the USB Drive from a Remote Computer**
- **Connecting to the USB Drive with Microsoft Network Settings**

USB Drive Requirements

The wireless modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown below.

Bus	Speed/Second
USB 1.1	12 Mbits
USB 2.0	480 Mbits

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

The wireless modem router should work with USB 2.0 or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the wireless modem router, go to: *http://kbserver.netgear.com/kb_web_files/n101300.asp*

When selecting a USB device, bear in mind the following:

- The USB port on the wireless modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- Per the USB 2.0 specification, the maximum available power is 5V @ 0.5A. Some USB devices may exceed this requirement, in which case the device may not function or may function erratically. Check the documentation for your USB device to be sure.
- The wireless modem router supports FAT, FAT32, NTFS (read only) and Linux file systems.

File Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any PC, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia with friends and family — sharing MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network — storing files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between the systems.
- Sharing files with offsite coworkers — sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Sharing Photos with Friends and Family

You can create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo sharing site.

To share files with your friends and family:

1. Insert your USB drive into the USB port on the wireless modem router either directly or with a USB cable.

   Computers on your local area network (LAN) can automatically access this USB drive using a Web browser or Microsoft Networking.

2. If you want to specify read only access, or to allow access from the Internet, see ***Configuring USB Storage Advanced Settings*** on page 94.

Storing Files in a Central Location for Printing

This scenario is for a family that has one high quality color printer directly attached to a PC, but not shared on the local area network (LAN). This family does not have a print server:

- The daughter has some photos on her Macintosh computer that she wants to print.
- The mother has a photo-capable color printer directly attached to her PC, but not shared on the network.
- The mother and daughter's computers are not visible to each other on the network.

How can the daughter print her photos on the color printer attached to her mother's PC? This is where the USB drive on the wireless modem router can save you time and effort.

1. The daughter accesses the USB drive by typing **\\readyshare** in the address field of her Web browser. Then she copies the photos to the USB drive.
2. The mother uses a her Web browser or Microsoft Networking to transfer the files from the USB drive to the PC. Then she prints the files.

Sharing Large Files with Colleagues

Sending files that are larger than 5 MB can pose a problem for many e-mail systems. The wireless modem router allows you to share very large files such as PowerPoint presentations or ZIP files with colleagues at another site. Rather than tying up their mail systems with large files, your colleagues can use FTP to easily download shared files from the wireless modem router.

Sharing files with a remote colleague involves the following steps:

1. To protect your network, set up appropriate security. Create a user name and password for the colleague with appropriate access.
2. If you want to limit USB drive access to only Read Access, from the wireless modem router USB Storage (Basic Settings) screen, click **Edit a Network folder**. In the Write Access field, select **admin**, and then click **Apply**.

Note: The password for admin is the same one that you use to access the wireless modem router. By default it is **password**.

3. Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See ***Configuring USB Storage Advanced Settings*** on page 94.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your wireless modem router. On the wireless modem router main menu below the USB heading, select Basic Settings. The following screen displays:

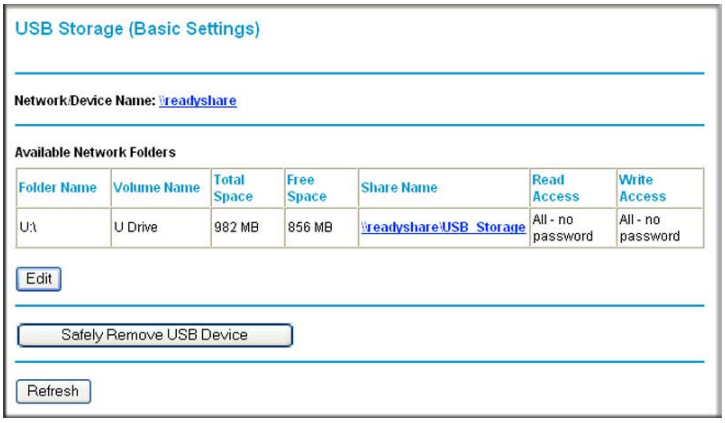


Figure 48.

By default, the USB storage device is available to all computers on your local area network (LAN). To access your USB device from this screen, you can click the **Network/Device Name** or the **Share Name**.

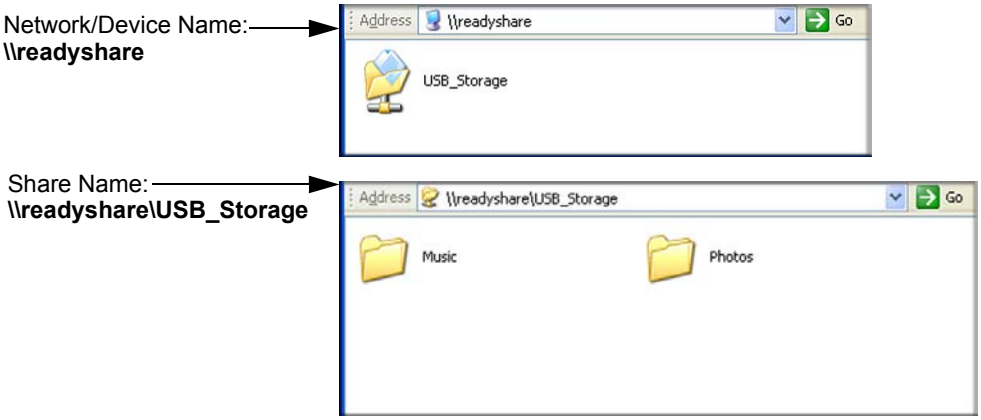


Figure 49.

You can also type **\\readyshare** in the address field of your Web browser.

Note: If you logged in to the wireless modem router before you connected your USB device, you might not see your USB device in the wireless modem router screens until you log out and then log back in again.

The following table explains the fields and buttons in this screen.

Fields and Buttons		Description
Network Device Name		The default is \\readyshare. This is the name used to access the USB device connected to the wireless modem router.
Available Network folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	Shows the current utilization of the storage device.
	Share Name	• You can click the name shown or you can type it in the address field of your Web browser. • If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
	Read/Write Access	• Shows the permissions/access controls on the network folder: • All -no password allows all users to access the network folder. • admin uses the same password that you use to log in to the wireless modem router main menu.
Edit button		You can click the **Edit** button to edit the Available Network folder settings. See ***Editing a Network Folder*** on page 93.
Safely Remove USB Device button		Click to safely remove the USB device attached to your wireless modem router. See ***Unmounting a USB Drive*** on page 97.

Editing a Network Folder

This process is the same from either the USB Storage (Basic Settings) screen or the USB Storage (Advanced Settings) screen. Click the **Edit** button to open the Edit Network Folder screen:

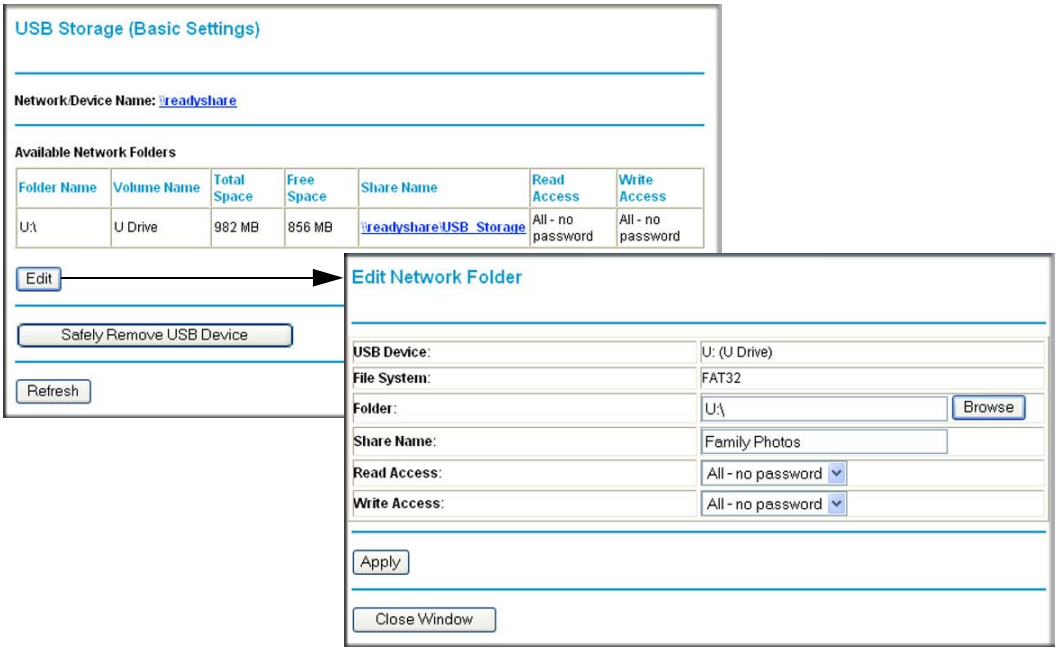


Figure 50.

You can use this screen to select a folder, to change the **Share Name**, or to change the **Read Access** or **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the wireless modem router main menu. By default it is **password**.

Note: You must click **Apply** in order for your changes to take effect.

Configuring USB Storage Advanced Settings

To configure advanced USB settings, under the USB heading on the wireless modem router main menu, select Advanced Settings. The USB Storage (Advanced Settings) screen displays:

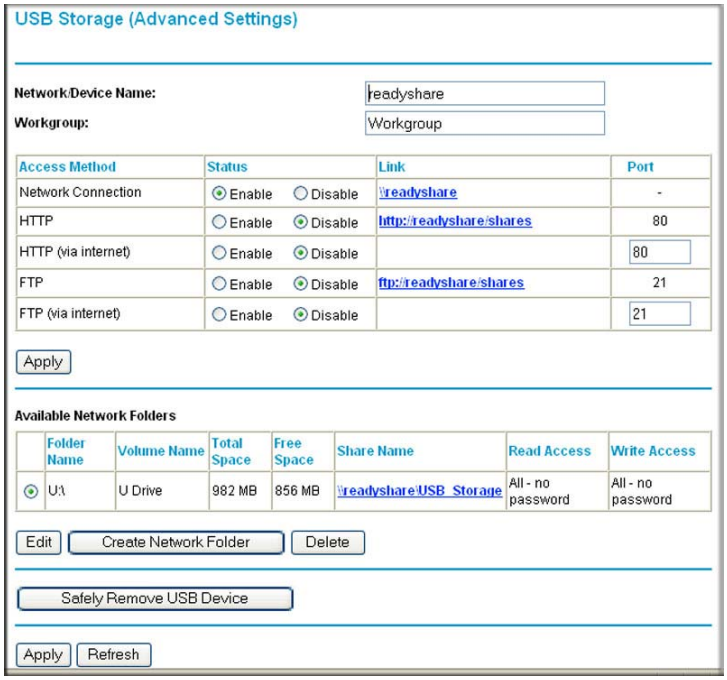


Figure 51.

You can use this screen to specify access to the USB storage device. The following table explains the fields and buttons in the USB Storage Advanced Settings screen.

Fields	Description
Network Device Name	The default is readyshare. This is the name used to access the USB device connected to the wireless modem router from your computer.
Workgroup	If you are using a Windows Workgroup rather than a domain, the Workgroup name is displayed here.

Fields		Description
Access Method	Network Connection	Enabled by default, this allows all users on the LAN to have access to the USB drive.
	HTTP	Disabled by default. If you enable this setting, you can type http://readyshare to access the USB drive.
	HTTP (via Internet)	Disabled by default. If you enable this settings, remote users can type http://readyshare to access the USB drive over the Internet.
	FTP	Disabled by default.
	FTP (via Internet)	Disabled by default. If you enable this settings, remote users can access the USB drive via ftp over the Internet.
Available Network Folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	The current utilization of the storage device.
	Share Name	• You can click the name shown or you can type it into the address field of your Web browser. • If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
	Read/Write Access	• Shows the permissions/access controls on the Network Folder: • All -no password allows all users to access the Network Folder. • admin prompts you to enter the same password that you use to log in to the wireless modem router main menu.

Creating a Network Folder

From the USB Storage (Advanced Settings) screen. Click the **Create a Network Folder** button to open the Create a Network Folder screen:

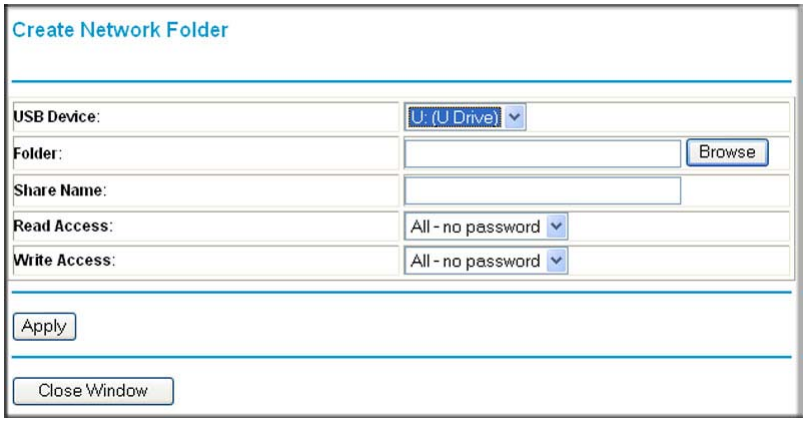


Figure 52.

You can use this screen to create a folder and to specify its **Share Name**, **Read Access**, and **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the wireless modem router main menu. By default it is **password**.

Note: You must click **Apply** in order for your changes to take effect.

Unmounting a USB Drive

WARNING!

Unmount the USB drive first before physically unplugging it from the wireless modem router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

Specifying Approved USB Devices

You can specify which USB devices are approved for use when connected to the wireless modem router.

1. Under the Advanced Heading, select USB Settings from the main menu, and then click **Approved Devices**. The USB Drive Approved Settings screen displays:

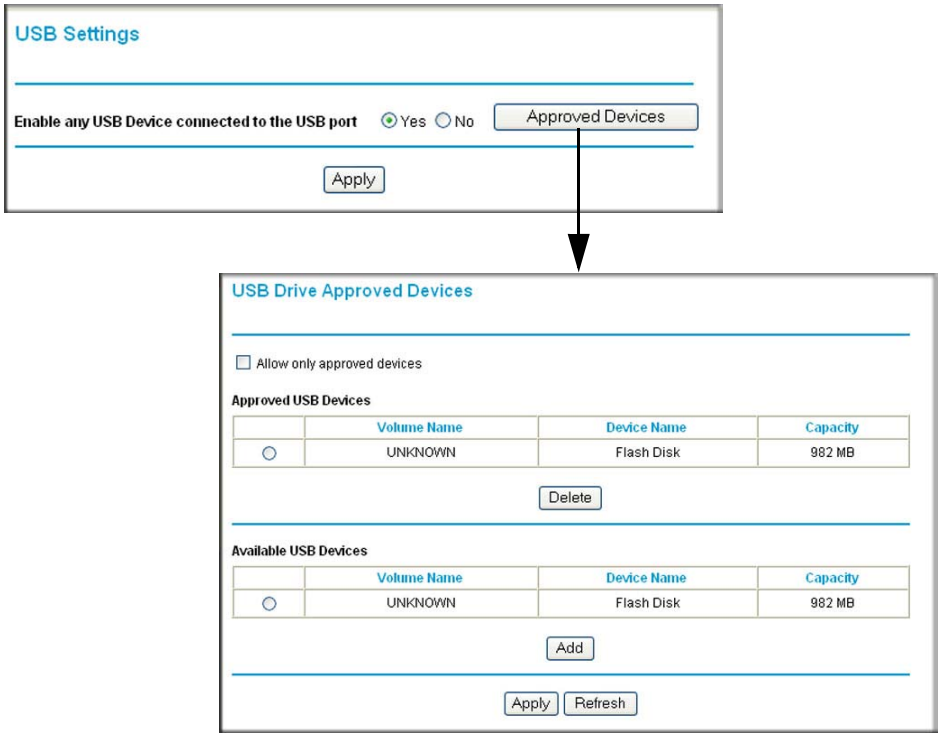


Figure 53.

2. Select the USB device from the **Available USB Devices** list.
3. Click **Add**.
4. Select the **Allow only approved devices** check box.
5. Click **Apply** so that your change goes into effect.

   If you want to approve another USB device, you must first use the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

Connecting to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you must use the router's Internet port IP address.

Locating the Internet Port IP Address

The Router Status screen shows the Internet port IP address:

1. Log in to the wireless modem router.
2. Under the Maintenance section in the left navigator, click **Router Status**.
3. Record the IP address that is listed for the Internet Port. This is the IP address you can use to connect to the router remotely.

Accessing the Router's USB Drive Remotely Using FTP

You can connect to the router's USB drive using a Web browser:

1. Connect to the router by typing ftp:// and the Internet port IP address in the address field of Internet Explorer or Netscape® Navigator, for example:

   ftp://10.1.65.4 If you are using dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the account name and password that has access rights to the USB drive.
3. The directories of the USB drive that your account has access to will be displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connecting to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You must be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as drag and drop, file open, or cut/paste files from:

- Microsoft Windows Start Menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer's network properties must be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networks must be enabled, as described below.

Note: In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

Configuring Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click Network Neighborhood and then click Properties. File and printer sharing for Microsoft Windows should be listed. If not, click Add and follow the installation prompts.

Note: **Note:** If you have any questions on File and Printer Sharing, please contact Microsoft for assistance.

Configuring Windows 2000 and Windows XP

Right-click on the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If not, click Install and follow the installation prompts.

Troubleshooting

7

This chapter provides information about troubleshooting your wireless modem router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?

  Go to **Basic Functioning**."
- Have I connected the router correctly?

  Go to **Basic Functioning**."
- I cannot access the router's configuration with my browser.

  Go to ***Cannot Log in to the N300 Wireless Modem Router*** on page 104.
- I have configured the router but I cannot access the Internet.

  Go to ***Troubleshooting the ISP Connection*** on page 105.
- I want to clear the configuration and start over again.

  Go to ***Restoring the Default Configuration and Password*** on page 111.
- I cannot remember the router's configuration password.

  Go to ***Factory Default Configuration*** on page 115.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify the following:
   a. The LAN port LEDs are lit for any local ports that are connected.
   b. The ADSL Link LED is lit.

   If the ADSL link LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.

   If any of these conditions does not occur, refer to the appropriate following section.

"Welcome" Page Displays instead of Router Management Interface

This situation can occur if the CD Setup Wizard does not complete successfully; the unit will stay in "Wizard Mode". If the "Welcome" page displays instead of the Router Management interface when you try to go to the Internet or log into the Router Management interface, you can bypass the wizard using one of the following methods:

- Log into the Router Management interface at **http://routerlogin.com/basicsetting.htm**.
- Perform a factory reset to take the router out of "Wizard Mode" altogether.

Power LED Is Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact Technical Support.

Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router. The Power LED also turns red when you press the Wireless On/Off and WPS buttons on the side panel of the router simultaneously for 6 seconds, and blinks red 3 times when you release these buttons. However, in this case, the wireless modem router is working normally.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the router recovers.

If the power LED is still red 1 minute after power up:

- Turn the power off and on to see if the router recovers.
- Clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in ***Using the Wireless On/Off and WPS Buttons to Reset the Router*** on page 111.

If the error persists, you might have a hardware problem and should contact Technical Support.

LAN or ADSL Port LED Is Not On

If either the LAN LEDs or ADSL Link LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable: when connecting the ADSL port, use the cable that was supplied with the wireless modem router. If the ADSL link LED is still off, this may mean that there is no ADSL service or the cable connected to the ADSL port is bad.

Window Appears Asking You to Reload Firmware

If a window appears with a message asking you to reload the firmware, this indicates that a problem has been detected with the current firmware. Please follow the on-screen instructions to access new firmware and reload the firmware into your router.

Cannot Log in to the N300 Wireless Modem Router

If you are unable to log in to the wireless modem router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Follow the instructions in the online document that you can access from ***Preparing Your Network*** on page 117 for information about how to configure your computer.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in ***Using the Wireless On/Off and WPS Buttons to Reset the Router*** on page 111.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

If the router does not save changes you have made, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

ADSL Link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

ADSL Link LED Is Green or Blinking Green

If your ADSL link LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

ADSL Link LED Is Blinking Amber

If your ADSL link LED is blinking amber, then your wireless modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

ADSL Link LED Is Off

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The wireless modem router uses pins 2 and 3.

Internet LED is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your log-in credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the Multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Check if your ISP has a problem—it may not be the router that cannot connect to the Internet but your ISP that cannot provide an Internet connection.

Obtaining an Internet IP Address

If your wireless modem router is unable to access the Internet, and your Internet LED is green or blinking green, you should determine whether the wireless modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the Internet IP address from the browser interface:

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the wireless modem router's configuration at http://192.168.0.1.
3. In the main menu, under Maintenance, select Router Status and check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your wireless modem router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, **Troubleshooting PPPoE or PPPoA**.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account to the wireless modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings screen. See the *N300 Wireless Gigabit ADSL2+ Modem Router DGN3500 Setup Manual*.

Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at http://192.168.0.1.
2. Under Maintenance, select **Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The wireless modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the wireless modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your wireless modem router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the wireless modem router's configuration, reboot your computer, and verify the DNS address as described in the online document that you can access from ***Preparing Your Network*** on page 117. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the wireless modem router configured as its TCP/IP wireless modem router.

  If your computer obtains its information from the wireless modem router by DHCP, reboot the computer, and verify the wireless modem router address as described in the online document that you can access from ***Preparing Your Network*** on page 117.

Resolving a 'Reload Firmware' Message

When you attempt to connect to the Internet, Windows may display a message that you must reload the router's firmware. If this situation occurs, a problem has been detected with the router's firmware.

To recover the firmware:

1. If you already have the firmware file on your PC, go directly to step 2. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at *http://www.netgear.com/support*.
2. Click **Browse**.
3. Navigate to the firmware file. (If you used the Setup CD, recovery firmware is located in the C:\Netgear directory.)
4. Click **Upgrade**.
5. The recovery process takes about 5 minutes. Wait for the progress bar to complete. After the firmware recovery is complete, the login screen for the Smart Wizard displays, allowing you to log in to the wireless modem router to check its status.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **Ping** followed by the IP address of the router, as in this example:

   ping 192.168.0.1
3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in ***LAN or ADSL Port LED Is Not On*** on page 103.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, type:

PING -n 10 IP address

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default wireless modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router as described in the online document that you can access from ***Preparing Your Network*** on page 117.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to your *N300 Wireless Gigabit ADSL2+ Modem Router DGN3500 Setup Manual*.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see ***Erasing the Configuration*** on page 61).
- The DGN3500 has a dedicated reset button located on the back panel. Press reset button for over 5 seconds. The LED will blink and the router will reboot. The factory default setting is restored after system boots up.

Using the Wireless On/Off and WPS Buttons to Reset the Router

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the Wireless On/Off and WPS buttons on the side panel of the router:

1. Press and hold the Wireless On/Off and WPS buttons simultaneously until the Power LED turns red (about 6 seconds).
2. The DGN3500 has a dedicated reset button located on the back panel. Press reset button for over 5 seconds. The LED will blink and the router will reboot. The factory default setting is restored after system boots up.

Problems with Date and Time

In the main menu, under Security, select Schedule to display the current date and time of day. The wireless modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000.
  Cause. The router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
  Cause. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

Technical Specifications

A

This appendix provides technical specifications for the wireless modem router.

- **General Specifications**
- **Factory Default Configuration**

General Specifications

Specification		Description
Network Protocol and Standards Compatibility		
	Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter		
	North America	120V, 60 Hz, input
	UK, Australia	240V, 50 Hz, input
	Europe	230V, 50 Hz, input
	All regions (output)	12 V AC @ 1.0A output
Physical		
	Dimensions	7.0" x 5.1" x 1.2" 177.5 mm x 130 mm x 31 mm
	Weight	0.58 lbs. 0.265 kg
Environmental		
	Operating temperature	0° to 40° C (32° to 104° F)
	Operating humidity	10% to 90% relative humidity, noncondensing
	Storage temperature	–20° to 70° C (–4° to 158° F)
	Storage humidity	5 to 95% relative humidity, noncondensing
Regulatory Compliance		
	Meets requirements of:	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx, RJ-45
	WAN	ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite
	USB	?

Factory Default Configuration

You can use the Restore Factory Settings button on the rear panel of the wireless modem router to return its configuration to the factory settings. This is called a hard reset. To perform a hard reset, press and hold the Restore Factory Settings button until the LEDs flash. Your wireless modem router restarts and returns to the factory configuration settings shown in the following table.

Feature		Default Behavior
Login		
	Modem Router user login URL	http://www.routerlongin.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
	ReadyShare Access	\\readyshare
Internet Connection		
	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	Autosensing
Local Network (LAN)		
	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2

Feature		Default Behavior
	DHCP ending IP address	192.168.0.254
	DMZ	Disabled
	Time zone	GMT
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless		
	Wireless communication	Enabled
	SSID name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission speed	Auto[1]
	Country/region	United States (in North America; otherwise, varies by region)
	RF channel	11 unit if region is selected
	Operating mode	Up to 130 Mbps (with 20/40 MHz bandwidth dynamically selected on a frame-by-frame basis)
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless card access list	All wireless stations allowed

1 Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Related Documents

B

This appendix provides links to reference documents that you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
TCP/IP Networking Basics	**http://documentation.netgear.com/reference/enu/tcpip/index.htm**
Wireless Networking Basics	**http://documentation.netgear.com/reference/enu/wireless/index.htm**
Preparing Your Network	**http://documentation.netgear.com/reference/enu/wsdhcp/index.htm**
Virtual Private Networking Basics	**http://documentation.netgear.com/reference/enu/vpn/index.htm**
Glossary	**http://documentation.netgear.com/reference/enu/glossary/index.htm**

Notification of Compliance

NETGEAR Wireless Routers

C

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the N300 Wireless Modem Router DGN3500 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, (N300 Wireless Modem Router DGN3500), does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Interference Reduction Table

Household Appliance	Recommended Minimum Distance between NETGEAR equipment and household appliance to reduce interference (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Europe – EU Declaration of Conformity

Marking with the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

This equipment meets the following conformance standards:

- EN300 328 (2.4Ghz), EN301 489-17, EN301 893 (5Ghz), EN60950-1
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.
- In Italy, the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
- This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.
- For complete DoC, visit the NETGEAR EU Declarations of Conformity website at: *http://kb.netgear.com/app/answers/detail/a_id/11621/*

EDOC in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Index

Numerics

128-bit WEP 25
64-bit WEP 25

A

access
  remote 63
  viewing logs 36
access lists 22
account name 55
address reservation 70, 74
ADSL settings 13
attached devices 59
authentication, required by mail server 49

B

backing up configuration file 60
basic wireless connectivity 17

C

compliance, wireless 118
configuration file 60
  backing up 60
  erasing 61
configuring
  dynamic DNS 76
connection status settings 57

D

date and time 112
daylight savings time 47, 112
default DMZ server 67
default factory settings
  restoring 61
default reset buttons 111
deleting configuration 61
Denial of Service (DoS) protection 37
device name 59
DHCP server 70, 73
diagnostics 62
DMZ server 67
DNS server
  primary DNS server 11
  secondary DNS server 11
dynamic DNS 76
DynDNS.org 76

E

e-mailing logs 49
erasing configuration 61
Ethernet MAC address. *See* MAC addresses

F

factory default settings
  restoring 61
firewall rules
  inbound rules 40
  order of precedence for firewall rules 44
  outbound rules 42
Firmware Upgrade Assistant 7
firmware version 55

H

host name 11, 55, 59

I

inbound firewall rules 40
instant messaging 44
interval, poll 58
IP addresses
  dynamic 76
  reserved 70, 74

L

LAN port
  settings 56
LAN setup 67, 68, 72
  default LAN IP configuration 68, 72

logging in 7
logging out 7
logs
    sending 49
    viewing 36

M

MAC address
    configuring the MAC address 12
    MAC address being rejected 110
    MAC address filter 23
    MAC address spoofing 106
    restricting wireless access by MAC address 24
MAC addresses
    attached devices 59
mail server, outgoing 49
managing router remotely 63
manual software upgrade 53
metric 79
multicasting 69, 73

N

Network Time Protocol 47, 112

O

order of precedence for firewall rules 44
outbound firewall rules 42
outgoing mail server 49

P

passphrase 25
placement of your router 15
plug and play 81
point-to-point bridge mode 84
poll interval 58
port status 58
ports
    port filtering 42
    port forwarding 40
    port numbers 45
primary DNS server 11

R

range of your wireless connection 15
releasing connection status 58
remote management 63
renewing connection status 57

repeater mode with wireless client association 85
reserved IP adresses 70, 74
reset button 111
restoring
  configuration 60
  default factory settings 61
restoring your password 111
restricting wireless access by MAC address 24
RIP (Router Information Protocol) 69, 73
router status, viewing 55

S

secondary DNS server 11
service blocking 42
service numbers 45
SMTP server 49
software, upgrading 52
SSID 19
status, router, viewing 55
system up time 58

T

TCP/IP network troubleshooting 109
technical support 2
time of day 112
time zone 47
timeout, administrator login 35
time-stamping 47
trademarks 2
troubleshooting
  general information 101
  network troubleshooting 109
  troubleshooting LEDs 103
trusted host 38

U

up time, system 58
updating firmware 7
upgrading router software 52
USB drive requirements 88
USB drive, unmounting 97

V

viewing
  attached devices 59
  logs 36
  router status 55

W

WEP authentication 24
wireless card access list 21
wireless encryption
    WEP encryption 24
    WPA encryption 26
wireless mode
    g & b 19
    g only 19
wireless security 16, 29